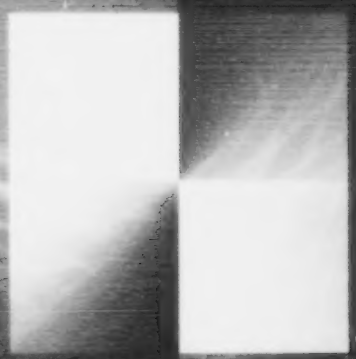
COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE

AVIS

VISER UN JUSTE ÉQUILIBRE

UN REGARD ÉTHIQUE SUR LES NOUVELLES TECHNOLOGIES DE SURVEILLANCE ET DE CONTRÔLE À DES FINS DE SÉCURITÉ



Québec

COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE

AVIS

VISER UN JUSTE ÉQUILIBRE

UN REGARD ÉTHIQUE SUR LES NOUVELLES TECHNOLOGIES DE SURVEILLANCE ET DE CONTRÔLE À DES FINS DE SÉCURITÉ

COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE

AVIS

VISER UN JUSTE ÉQUILIBRE

UN REGARD ÉTHIQUE SUR LES NOUVELLES TECHNOLOGIES DE SURVEILLANCE ET DE CONTRÔLE À DES FINS DE SÉCURITÉ

Québec

Commission de l'éthique de la science et de la technologie

1200, route de l'Église
3e étage, bureau 3.45
Québec (Québec)
G1V 4Z2
www.ethique.gouv.qc.ca

En soutien à la réalisation de l'avis

Coordination et supervision

Diane Duquet et Nicole Beaudry

Secrétaire de réunion

David Boucher

Recherche et rédaction

David Boucher et Diane Duquet

Soutien technique

Secrétariat

Annie St-Hilaire

Documentation

Monique Blouin et Annie Lachance

Communication et supervision de l'édition

Guillaume Huet

Révision linguistique

Le Graphe

Conception de la page couverture

Création Sylvain Vallières inc.

Conception et mise en pages

Éditions MultiMondes

Impression

Imprimerie Le Laurentien

Avis adopté à la 34e réunion de la Commission de l'éthique de la science et de la technologie le 12 février 2008

© Gouvernement du Québec 2008
Dépôt légal : 2008
Bibliothèque nationale du Québec
Bibliothèque nationale du Canada
ISBN 978-2-550-52239-3

Pour faciliter la lecture du texte, le genre masculin est utilisé sans aucune intention discriminatoire.

Les membres du Comité de travail

Président

BENOIT GAGNON
Chercheur associé
Chaire de recherche du Canada en sécurité, identité et technologie
Doctorant à l'Université de Montréal

Membres

FRÉDÉRIC ABRAHAM
Doctorant en philosophie
Université du Québec à Trois-Rivières

PATRICK BEAUDIN
Directeur général
Société pour la promotion de la science et de la technologie

M[e] EDITH DELEURY
Présidente de la CEST
Faculté de droit
Université Laval

BENOIT DUPONT
Titulaire de la Chaire de recherche du Canada en sécurité, identité et technologie
Professeur
École de criminologie
Université de Montréal

FREDERICK GAUDREAU, lt
Coordonnateur
Module de la cybersurveillance et de la vigie
Sûreté du Québec

STÉPHANE LEMAN-LANGLOIS
Chercheur régulier
Centre international de criminologie comparée (CICC)
Professeur
École de criminologie
Université de Montréal

M[e] DANIELLE PARENT
Directrice des affaires juridiques
Bureau du Commissaire au lobbyisme du Québec

M[e] MARIE-CLAUDE PRÉMONT
Professeure de droit
École nationale d'administration publique (ÉNAP)

SERGE TRUDEL
Directeur dossier de l'Accès à l'information/éthique
Association canadienne de la sécurité (CANASA)

DANIEL MARC WEINSTOCK
Titulaire de la Chaire de recherche du Canada en éthique et en philosophie politique
Professeur
Département de philosophie
Université de Montréal

Membre observateur

RAYMOND D'AOUST
Commissaire adjoint
Commissariat à la protection de la vie privée du Canada

Du secrétariat de la Commission

M[e] Nicole Beaudry, coordonnatrice de la CEST
David Boucher, conseiller en éthique et secrétaire du comité de travail

Conseil de la science
et de la technologie
Québec

Mars 2008

Monsieur Raymond Bachand
Ministre
Ministère du Développement économique
de l'Innovation et de l'Exportation
710, place d'Youville, 6e étage
Québec (Québec) G1R 4Y4

Monsieur le Ministre,

Je vous transmets par la présente la version finale de l'avis intitulé *Pour un encadrement éthique et un regard citoyen sur les nouvelles technologies de surveillance et de contrôle social*, préparé par la Commission de l'éthique de la science et de la technologie.

Espérant le tout à votre entière satisfaction, je vous prie d'accepter, Monsieur le Ministre, l'expression de ma haute considération.

Les présidents,

Marie-France Germain

Commission
de l'éthique
de la science
et de la technologie
Québec

Québec, le 3 mars 2007

Madame Marie-France Germain
Présidente
Conseil de la science et de la technologie
1200, route de l'Église
3e étage, bureau 3.45
Québec (Québec) G1V 4Z2

Madame la Présidente,

Il me fait plaisir de vous remettre l'Avis au ministre du Développement économique, de l'Innovation et de l'Exportation intitulé *Viser un juste équilibre : Un regard éthique sur les nouvelles technologies de surveillance et de contrôle à des fins de sécurité*.

Je vous prie de recevoir, Madame la Présidente, mes salutations distinguées.

La présidente de la Commission de l'éthique
de la science et de la technologie.

Édith Deleury

Table des matières

Liste des sigles xvii

Résumé et recommandations xix

INTRODUCTION 1

CHAPITRE I – LE DÉPLOIEMENT DES NOUVELLES TECHNOLOGIES DE SURVEILLANCE ET DE CONTRÔLE À DES FINS DE SÉCURITÉ : UN PHÉNOMÈNE EN CONTINUITÉ AVEC LA MODERNITÉ 3

La sécurité : une notion à préciser 3

Le sentiment d'insécurité : une réalité difficile à cerner 4

Le rôle des médias 4

Le rôle politique de la peur du crime 5

Quelle est l'ampleur du sentiment d'insécurité et que craint-on ? 5

La place du risque dans la société 8

Qu'est-ce que le risque ? 8

Les caractéristiques de la « société du risque » 9

Vers une société de surveillance ? 11

Qu'est-ce que la surveillance ? 12

Les caractéristiques de la société de surveillance 13

Le cadre éthique : les enjeux et les valeurs en cause 14

Les valeurs 14

Les enjeux éthiques 16

Les espaces publics et privés : une frontière ténue 17

Les instruments normatifs en place 17

La définition juridique du renseignement personnel 17

La protection de la vie privée et des renseignements personnels à l'échelle québécoise 18

La protection de la vie privée et des renseignements personnels à l'échelle canadienne 20

La protection de la vie privée et des renseignements personnels à l'échelle régionale et internationale 21

CHAPITRE 2 – LES NOUVELLES TECHNOLOGIES DE SURVEILLANCE ET DE CONTRÔLE : UN TOUR D'HORIZON 23

Les systèmes biométriques : obéir au doigt et à l'œil ? 23

Quelques définitions utiles 23

Les finalités associées à l'utilisation des données biométriques 24

Les différentes technologies actuelles et en développement et leur mode de fonctionnement 25

Les atouts des technologies biométriques 26

Les failles des technologies biométriques 27

Le marché de la biométrie 29

L'intérêt de la population 30

La vidéosurveillance : l'œil omniprésent 31

Quelques définitions utiles 32

Les secteurs d'utilisation de la vidéosurveillance 33

Les différentes technologies actuelles et en développement et leur mode de fonctionnement 33

Les atouts de la vidéosurveillance 34

Les failles de la vidéosurveillance 34

Le marché de la vidéosurveillance 35

L'intérêt de la population 35

L'identification par radiofréquence (IRF) : vers l'intelligence ambiante ? 35

Quelques définitions utiles 36

Les finalités associées à l'IRF 36

Les différentes technologies actuelles et en développement et leur mode de fonctionnement 36

Les atouts de l'IRF 37

Les failles de l'IRF 38

Le marché de l'IRF 38

L'intérêt de la population 39

CHAPITRE 3 – UN REGARD ÉTHIQUE SUR LES NOUVELLES TECHNOLOGIES DE SURVEILLANCE ET DE CONTRÔLE : À LA RECHERCHE D'UN JUSTE ÉQUILIBRE ENTRE LES VALEURS 41

L'évaluation de la pertinence, de l'efficacité et de la fiabilité des NTSC : une étape préalable 42

La proportionnalité de la réponse à l'insécurité : pour un déploiement modéré 42

L'acceptabilité sociale : une condition essentielle 44

Le consentement : un concept difficilement transposable dans le contexte des NTSC 44

Le respect des finalités : un principe à réaffirmer 47
Des préoccupations en lien avec le cadre normatif 47
Des préoccupations en lien avec les différentes NTSC 48
Des préoccupations en lien avec la conservation des données 49
Des préoccupations en lien avec les risques de discrimination et de stigmatisation 49
La protection des renseignements personnels : pour des conduites respectueuses de la vie privée 50
Données biométriques 50
Vidéosurveillance 52
Identification par radiofréquence 52
Le traitement automatisé de l'information : une pratique qui soulève des inquiétudes 54
Le transfert transfrontalier de renseignements personnels 54
CONCLUSION 57
Glossaire 61
Bibliographie 63
ANNEXE 1 – LES RÈGLES D'UTILISATION DE LA VIDÉOSURVEILLANCE AVEC ENREGISTREMENT DANS LES LIEUX PUBLICS PAR LES ORGANISMES PUBLICS 69
ANNEXE 2 – LIGNES DIRECTRICES DU COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA CONCERNANT LE RECOURS, PAR LES FORCES POLICIÈRES ET LES AUTORITÉS CHARGÉES DE L'APPLICATION DE LA LOI, À LA SURVEILLANCE VIDÉO DANS LES LIEUX PUBLICS 73
LES ACTIVITÉS DE CONSULTATION ET D'INFORMATION DE LA COMMISSION 77
LISTE DES MEMBRES DE LA COMMISSION 79

Liste des sigles et acronymes

AAPI :	Association sur l'accès et la protection de l'information
ADN :	Acide désoxyribonucléique
CAI :	Commission d'accès à l'information (Québec)
CANASA :	Association canadienne de la sécurité
CCNE :	Comité consultatif national d'éthique pour les sciences de la vie et de la santé (France)
CNIL :	Commission nationale de l'informatique et des libertés (France)
IRF :	Identification par radiofréquence
NTSC :	Nouvelles technologies de surveillance et de contrôle
OCDE :	Organisation de coopération et de développement économiques
ONU :	Organisation des Nations Unies

Résumé et recommandations

La surveillance de masse peut être considérée comme un trait caractéristique des sociétés modernes. Son importance n'a d'égal que les moyens mis en place pour amasser des renseignements. Parmi ces moyens, les nouvelles technologies de surveillance et de contrôle (NTSC) et surtout les manières de les déployer soulèvent des enjeux éthiques. Aussi la Commission de l'éthique de la science et de la technologie s'est-elle donné le mandat de formuler un avis sur des technologies pouvant servir à la surveillance de masse à des fins de sécurité : les systèmes biométriques, la vidéosurveillance et l'identification par radiofréquence (IRF).

La Commission tient à préciser qu'elle voulait traiter des NTSC sous l'angle de leurs applications à des fins de sécurité, ce qui excluait notamment les fins de surveillance sur les lieux de travail, les fins associées à la santé et les applications liées à la gestion des inventaires. Mais qu'est-ce que la sécurité ? Poser la question met déjà en évidence la complexité du concept. En effet, non seulement le terme renvoie à différentes notions, notamment sur le plan sociologique, mais son interprétation varie en fonction des langues, des discours, des approches et de l'histoire.

Assurer la sécurité d'un territoire, d'un pays, d'une ville, d'une habitation est un défi constant, car il faut, d'une part, déterminer correctement les menaces et, d'autre part, mettre en place un système efficace de protection. À l'heure actuelle, et surtout depuis les événements du 11 septembre 2001, les paramètres du danger et de la sécurité semblent entièrement nouveaux et paraissent exiger l'adoption de mesures également nouvelles sur le plan tant technique que politique. Les NTSC sont l'une de ces nouvelles mesures.

Histoire de camper sa réflexion dans un contexte social, politique et éthique élargi, la Commission s'est interrogée dans un premier temps sur les liens susceptibles d'exister entre le déploiement des NTSC et certains phénomènes comme le sentiment d'insécurité par rapport à la criminalité et l'importance grandissante des notions de risque et de surveillance.

Tout d'abord, la Commission désirait y voir plus clair quant au sentiment d'insécurité auquel il est souvent fait référence dans les médias. Il s'avère en fait que le sentiment que les gens ont de leur propre sécurité dépend de plusieurs facteurs et qu'il peut être influencé par différents acteurs. Par conséquent, il s'agit d'une réalité plutôt difficile à cerner. Pour tenter de mieux évaluer l'ampleur réelle du sentiment d'insécurité, la Commission a examiné plusieurs enquêtes et sondages sur le sujet. Selon les données analysées il peut être conclu que les Canadiens et les Québécois se sentent en sécurité. La place qu'occupe dans les médias la couverture des actes criminels et terroristes ne refléterait donc aucunement les préoccupations de la population interrogée. De plus, une forte peur du crime viendrait en contradiction avec les statistiques sur la criminalité, du moins au Canada, qui font état d'un recul de la criminalité depuis quelques années.

Une société qui est alimentée, volontairement ou non, par une certaine insécurité est plus encline à exprimer un besoin constant d'informations pour évaluer et gérer les risques et les dangers qui la guettent. Plusieurs penseurs estiment que le fait d'être obsédé par les risques, les menaces et les dangers est un symptôme de l'insécurité qui affecte une société. C'est d'ailleurs pourquoi des auteurs, comme le sociologue Ulrich Beck, qualifient ces sociétés de sociétés du risque. Parmi les caractéristiques des sociétés du risque à mentionner, le besoin d'information de ses gestionnaires, mais aussi des citoyens, est particulièrement pertinent dans le cadre de l'avis de la Commission. Car, selon les théoriciens de la société du risque, plus l'information dont les personnes disposent est grande, plus ils sont en mesure de calculer, d'analyser et de gérer les risques dans l'espoir de les réduire, voire de les éliminer. Lorsque ce principe est appliqué au domaine de la sécurité, il devient évident pour la Commission que les NTSC constituent un puissant moyen de collecte d'informations servant à contrecarrer les menaces à la sécurité et à réduire la criminalité. Sans affirmer que l'attrait pour les NTSC se

réduit à ces seules logiques, la Commission n'en estime pas moins qu'il s'agit là d'un des moteurs derrière le déploiement des NTSC à des fins de sécurité.

La collecte d'informations est, par conséquent, absolument vitale pour la société du risque. Ces informations sont obtenues, entre autres, par la surveillance. Mais la surveillance ne constitue pas un phénomène nouveau, car elle n'a pas attendu l'avènement d'une société du risque ou de technologies raffinées pour se manifester. La surveillance est reconnue comme partie intégrante de toutes les sociétés humaines depuis des temps immémoriaux, puisque le simple acte de socialisation serait impensable sans la surveillance exercée par les adultes. Récemment, et surtout en réaction aux événements du 11 septembre 2001, un changement de cap est observable dans les méthodes de collecte de renseignements. L'objet de la surveillance ne se limite plus à quelques segments de la population déjà considérés comme « à risque ». C'est maintenant la population en général qui est placée sous surveillance afin de cibler des interventions vers les personnes jugées à risque ou qui posent des risques pour d'autres personnes.

Ce n'est pas vraiment l'apparition imminente d'un *Big Brother* qui inquiète la Commission. En fait, c'est l'avènement de nombreux *Small Brothers*, c'est-à-dire de plusieurs organismes et personnes qui, à titre privé, se mettent à faire de la surveillance à des fins de sécurité, qui est préoccupant. Ce genre de surveillance qui ne respecte pas nécessairement toujours les lignes directrices et les bonnes pratiques en la matière risque d'échapper totalement au contrôle de l'État.

Prenant appui sur ces éléments de contexte, la Commission définit ensuite le cadre éthique dans lequel elle s'inscrit pour porter un regard éthique sur les NTSC. Au regard des valeurs, la Commission souligne son attachement aux valeurs fondamentales au sein des sociétés démocratiques et plus particulièrement à la valeur d'autonomie. Dans les sociétés démocratiques libérales, cette valeur joue en effet un rôle central. L'autonomie est cette valeur qui permet aux personnes de mener et d'accomplir un projet de vie comme bon leur semble, dans les limites imposées par les droits et libertés des autres personnes. Dans le présent avis, elle est conçue comme l'expression de la liberté des citoyens des sociétés démocratiques, notamment par rapport au regard, qui peut parfois être intrusif, de l'État et d'autres organisations. En outre, la Commission estime que plus les citoyens participeront à l'élaboration, à la mise en place et au suivi des balises entourant le déploiement des NTSC, plus ce processus sera conforme à l'idéal démocratique et respectera la valeur d'autonomie.

Cette volonté de privilégier l'autonomie des personnes dans les démocraties libérales se matérialise plus concrètement par l'attachement à toute une constellation de valeurs fondamentales. Bien que ces valeurs puissent, dans certains cas précis, entrer en conflit, il convient de reconnaître qu'elles ont un point commun. Elles rendent possibles l'autonomie et, partant, la vie démocratique. Parmi cet ensemble de valeurs, la Commission a retenu celles qu'elle estimait les plus concernées par le déploiement des NTSC, c'est-à-dire la sécurité, la liberté, la vie privée, la transparence, la justice et l'égalité. La Commission met ainsi l'accent sur le fait que le recours aux NTSC ne doit jamais faire abstraction de son objectif primordial : protéger les sociétés démocratiques contre les risques d'atteinte à leurs valeurs fondamentales. En cherchant à assurer une trop grande sécurité, les moyens de surveillance peuvent en effet menacer le respect des valeurs fondamentales des sociétés démocratiques. Le but de la Commission, avec le présent avis, est donc de viser un juste équilibre entre la sécurité et les droits et libertés individuels dans la protection des valeurs fondamentales des sociétés démocratiques.

Sur le plan technique, la Commission fournit une description détaillée des trois NTSC qui ont retenu son attention.

Un **système biométrique** permet d'identifier une personne ou vérifie l'admissibilité d'une personne « à se voir reconnaître certains droits ou services (notamment l'accès) basés sur la reconnaissance de particularités physiques (empreintes digitales, iris de l'œil, contour de la main...), de traces (ADN, sang, odeurs) ou d'éléments comportementaux (signature, démarche)[1] ». Les applications des systèmes biométriques sont encore plutôt rares.

1. Définition de la Commission nationale de l'informatique et des libertés (CNIL – France), rapportée dans OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, *Les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre*, France, Assemblée nationale, 2003, p. 8.

La **vidéosurveillance** consiste en la surveillance à distance de lieux publics ou privés, à l'aide de caméras le plus souvent motorisées, qui transmettent les images saisies à un équipement de contrôle qui les reproduit sur un écran. Dans ce cas, il s'agit d'une technologie de surveillance et de contrôle beaucoup plus répandue et familière. Il est toutefois moins certain que les plus récentes avancées technologiques en la matière, comme la numérisation et le couplage avec des logiciels de reconnaissance faciale, soient aussi connues.

L'**identification par radiofréquence** (IRF ou RFID), sans être véritablement une nouvelle technologie, trouve à l'heure actuelle des applications surprenantes, et cela, dans divers domaines. Deux composantes principales rendent l'IRF possible. Tout d'abord, une puce dotée « d'un circuit électronique qui stocke des données et une antenne qui communique les données au moyen d'ondes radio[2] ». Cette puce communique avec un lecteur, lequel possède « une antenne et un démodulateur qui traduit l'information analogique [...] en données numériques. L'information numérique peut alors être traitée par un ordinateur.[3] » En matière de sécurité, l'insertion de puces contenant des renseignements personnels ou d'autres informations (la nationalité, le sexe, la date de naissance, etc.) dans les documents d'identité et les cartes d'accès est la principale application de l'IRF. Pouvant être lues à distance, ces puces permettraient de suivre des personnes à la trace et de sécuriser des documents afin d'éviter la fraude et le vol d'identité.

Le déploiement des NTSC soulève plusieurs enjeux éthiques. La Commission a retenu quelques-uns d'entre eux pour en faire une analyse plus approfondie.

L'évaluation de la pertinence, de l'efficacité et de la fiabilité des NTSC

Pour assurer la légitimité de leur déploiement, la Commission estime que les nouvelles technologies de surveillance et de contrôle doivent être pertinentes, efficaces et fiables. Le critère de pertinence consiste à savoir si les NTSC s'avèrent le meilleur moyen pour répondre au besoin reconnu en matière de sécurité. Ainsi, d'autres moyens moins intrusifs sur le plan de la vie privée devraient être privilégiés. Pour que les NTSC soient efficaces, il faut que les résultats obtenus par leur déploiement correspondent aux visées d'origine. De plus, les NTSC doivent être fiables, c'est-à-dire qu'il faut éviter que leur fonctionnement ne soulève plus de problèmes qu'elles n'apportent de solutions. Pour être en mesure de justifier leur déploiement, il faudrait que les NTSC atteignent un niveau plus élevé de pertinence, d'efficacité et de fiabilité. La Commission estime également nécessaire de rappeler l'importance de déployer des technologies efficaces et fiables afin d'éviter de causer des préjudices à des personnes innocentes. Ces questions, bien qu'elles soient d'ordre plus technique, appellent des réponses dans lesquelles la valeur de transparence vis-à-vis la population occupe une place prépondérante. L'évaluation de l'efficacité des NTSC doit être aussi transparente que possible afin de permettre aux citoyens d'avoir l'heure juste à ce sujet. La Commission désire aussi mettre en garde contre le déploiement de technologies perçues comme fiables et qui contribueraient à répandre un faux sentiment de sécurité dans la population.

La proportionnalité de la réponse à l'insécurité

La Commission est préoccupée par l'ampleur que pourrait prendre un déploiement des NTSC qui se ferait l'écho d'une demande insatiable de sécurité. La mise en place de NTSC doit tenir compte des enjeux éthiques en la matière et chercher à atteindre un niveau de sécurité jugé acceptable, sans verser dans la surenchère sécuritaire. Il y a donc des ponts à établir entre les divers acteurs du milieu et la population afin d'en arriver à des consensus sur le sujet.

Avec le Comité consultatif national d'éthique pour les sciences de la vie et de la santé (CCNE), la Commission estime que la notion de proportionnalité des moyens doit être prise en considération, non seulement dans le cadre des systèmes biométriques, mais dans le déploiement des NTSC en général. Mettre en place des moyens de surveillance trop intrusifs sur le plan de la vie privée compte tenu des fins visées et du contexte, tout comme intégrer des données personnelles au-delà de ce qui est

2. GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL DU PARLEMENT EUROPÉEN ET DU CONSEIL, *Document de travail sur les questions de protection des données liées à la technologie RFID (radio-identification)*, Bruxelles, 2005, p. 3 et 4. [http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_fr.pdf].

3. *Ibid.*

nécessaire à la finalité déclarée, ne serait pas acceptable sur le plan éthique. Aussi la Commission invite-t-elle les décideurs politiques et privés à procéder à une évaluation et à une interprétation nuancées et lucides des besoins en matière de NTSC à des fins de sécurité.

Il est primordial que l'évaluation du rapport entre la fiabilité technique, la proportionnalité de la réponse à l'insécurité et le degré d'intrusion dans la vie privée soit faite pour chaque projet de déploiement de NTSC. Il apparaît qu'une telle évaluation serait à même de permettre un regard éthique sur les finalités pour lesquelles les NTSC sont concrètement mises en œuvre. Une telle procédure serait inédite et elle aurait pour avantage indéniable de positionner le Québec comme un meneur sur le plan de l'évaluation éthique des utilisations de ce type de technologies.

Par ailleurs, au cœur de l'évaluation de la proportionnalité de la réponse à l'insécurité se trouvent des acteurs trop souvent ignorés par les décideurs publics et privés : les fournisseurs et les installateurs de NTSC. Ces acteurs se situent sur la première ligne en ceci qu'ils doivent assurer les besoins d'organisations publiques et privées et de citoyens en matière de sécurité sur le plan technique. En plus d'être en mesure de bien conseiller leurs clients en matière de NTSC, ces acteurs doivent pouvoir répondre à cette question : Quelle technologie conviendrait pour assurer un degré de sécurité donné ? En d'autres mots, quel système de sécurité est-il recommandé d'installer en fonction du degré de sécurité qu'il faut assurer ? Les fournisseurs et les installateurs sont les premiers confrontés aux enjeux éthiques mentionnés par la Commission. Aussi est-il nécessaire qu'ils soient sensibilisés à ces questions pour que le déploiement des NTSC se fasse en accord avec les valeurs privilégiées. La question centrale semble être de savoir comment parvenir à une proportionnalité dans la réponse à l'insécurité dans un contexte de marché en croissance très rapide et où la logique du profit l'emporte souvent sur la logique éthique. De telles considérations invitent à une réflexion approfondie sur la régulation des NTSC. Or, de récents développements sur le plan législatif permettraient de diffuser le fruit de cette réflexion parmi les acteurs du milieu.

Au Québec, la nouvelle Loi sur la sécurité privée encadre notamment « les activités reliées aux systèmes électroniques de sécurité, soit l'installation, la réparation, l'entretien et la surveillance continue à distance de systèmes d'alarme contre le vol ou l'intrusion, de systèmes de surveillance vidéo ou de systèmes de contrôle d'accès, à l'exception d'un système sur un véhicule routier [...][4] ». La Loi précise entre autres que le futur Bureau de la sécurité privée dispensera de la formation aux représentants des titulaires de permis d'agence et que le gouvernement pourra, par règlement, déterminer quelle est la formation nécessaire pour l'utilisation d'équipement ou décider de la formation à exiger pour la délivrance d'un permis d'agent[5]. Cette formation devrait prévoir un volet obligatoire sur les enjeux éthiques. C'est pourquoi :

la Commission recommande que la formation dispensée par le Bureau de la sécurité privée aux représentants des titulaires de permis d'agence inclue un volet éthique obligatoire qui s'inspirera des enjeux éthiques soulevés dans le présent avis et que le gouvernement, conformément à la Loi sur la sécurité privée, adopte la réglementation nécessaire pour que la formation exigée pour la délivrance d'un permis d'agent prévoie également un tel volet éthique.

L'acceptabilité sociale

Il est difficile de déterminer le véritable niveau d'acceptabilité sociale du déploiement des NTSC. Une meilleure connaissance des perceptions et des opinions de la population en cette matière contribuerait certainement à y voir plus clair. Il est important que soient mieux connues les perspectives des citoyens à l'égard des NTSC. Il apparaît primordial de donner la parole à celles et ceux qui seront placés sous surveillance afin de favoriser un déploiement acceptable pour la société et accepté par elle.

En considérant la popularité actuelle des gouvernements qui font de la sécurité leur cheval de bataille et à la lumière des résultats de sondages et d'enquêtes sur l'acceptation des NTSC par la population, il semble que le déploiement des NTSC ne soit pas contraire à la volonté populaire. La Commission s'interroge toutefois sur le niveau de connaissance du public en matière de biométrie, de vidéosurveillance et d'identification par radiofréquence (IRF). Aussi toute forme de consultation sur les NTSC doit-elle faire une place importante à la population en général et chercher d'abord et avant tout à recueillir des opinions éclairées.

4. L.R.Q., chapitre S-3.5, 2006, c. 23, a. 1.
5. L.R.Q., chapitre S-3.5, 2006, c. 23, a. 41, 111 et 112.

Le consentement

La plupart du temps, il est tout simplement impossible pour les personnes surveillées de consentir à ce qu'il en soit ainsi. En fait, le consentement libre et éclairé, sur une base individuelle, n'est tout simplement pas un concept opérationnel lorsque vient le temps de l'appliquer aux NTSC. Cela ne signifie pas pour autant qu'un tel état de fait ne soulève pas de questions d'ordre éthique, au contraire.

Des données biométriques peuvent en effet être recueillies à l'insu des personnes, des caméras de surveillance peuvent capter des images dans une rue d'un centre-ville sans que tous les passants y aient consenti, l'implantation d'une puce d'IRF sous-cutanée peut s'avérer presque impossible à refuser pour certaines catégories de personnes. Différentes dispositions légales encadrent le consentement à la collecte et à la communication des renseignements personnels recueillis par des NTSC. Cependant, certaines de ces dispositions comportent des limites. La Commission insiste donc sur la nécessité de mettre en place des moyens permettant aux citoyens de faire valoir leurs doléances, le cas échéant, et que celles-ci soient prises en considération.

En outre, la Commission estime que les citoyens devraient être mieux informés notamment et non exclusivement à l'égard des points suivants :

- les dispositions juridiques entourant le déploiement des NTSC, la collecte, l'utilisation, la communication et la conservation des renseignements personnels ;
- les risques, les inconvénients, les avantages et les bénéfices potentiels entraînés par le déploiement des NTSC ;
- les lieux et les documents soumis à la surveillance ;
- les moyens mis à la disposition des citoyens pour qu'ils participent au déploiement des NTSC, ce qui favoriserait un processus ouvert et transparent ;
- les moyens mis à la disposition des citoyens pour qu'ils fassent connaître leur opinion en la matière, voire leurs plaintes, que ce soit sur le déploiement des NTSC en général ou sur un projet de déploiement de NTSC en particulier.

Dans l'esprit du principe de représentativité, en vertu duquel ce sont des élus qui prennent les décisions politiques et non l'ensemble des citoyens, la Commission estime que, si le déploiement des NTSC se fait de manière transparente et en accord avec les valeurs fondamentales des sociétés démocratiques, chaque individu n'a pas nécessairement à donner son consentement. Il est cependant essentiel de réunir certaines conditions permettant d'éclairer le processus qui mène au déploiement des NTSC et de donner toute la marge de manœuvre nécessaire aux opposants et aux critiques afin que ceux-ci puissent exprimer leur point de vue.

En lien avec l'enjeu du consentement, la Commission tient à mettre en garde les citoyens quant au caractère invisible du déploiement des NTSC. L'objectif de plusieurs promoteurs des NTSC est d'ailleurs d'intégrer ces technologies dans l'environnement en les camouflant. Selon la Commission, cette façon de faire peut avoir des répercussions sur l'autonomie des citoyens et sur le respect de leur vie privée.

Le respect des finalités

Le respect des finalités explicitées pour lesquelles les NTSC sont déployées et l'exploitation de toutes les utilisations possibles de ces dernières sont source de tensions. D'une part, le respect des finalités explicitées est un principe important qui tend à prévenir les détournements d'usage et certaines formes d'abus et de dérives. D'autre part, l'exploitation de toutes les utilisations possibles des NTSC (y compris des fins auxquelles les personnes n'ont pas consenti) permettrait probablement d'accroître la sécurité.

Devant les exemples portés à son attention, la Commission s'inquiète des glissements qu'elle observe et de ceux qui risquent de se produire dans un avenir rapproché. Des normes, des procédés, des pratiques, des moyens de surveillance et de contrôle mis en place dans la foulée d'attentats terroristes sont progressivement intégrés à la lutte à la petite délinquance, puis ils sont récupérés par le secteur commercial. À l'inverse, des technologies comme l'IRF (identification par radiofréquence), dont les applications sont souvent associées au commerce de détail et à la gestion des inventaires, semblent vouloir coloniser le domaine de la sécurité. Aussi, considérant la facilité avec laquelle les NTSC trouvent des applications et donc les finalités qui peuvent être très différentes, il convient de rester vigilant à cet égard.

La durée de conservation des données collectées par les NTSC constitue un paramètre important dans les risques de détournement d'usage. Le principe est simple : moins longtemps les données sont conservées, moins les risques de détournement d'usage sont grands. Par conséquent, il est important de prévoir la durée de conservation des enregistrements avant la mise en place d'un système de surveillance, cette durée ne devant pas excéder la durée normale de conservation nécessaire dans le cadre de la fin visée.

Enfin, la Commission veut attirer l'attention sur le fait que l'analyse des renseignements personnels recueillis par les NTSC comporte des risques en matière de discrimination et de stigmatisation. Étant donné la nature des renseignements personnels recueillis et la possibilité d'en extraire des informations sur l'origine ethnique et sur la santé des usagers, sur les habitudes de consommation et leur affiliation avec des partis politiques, la question des risques de discrimination et de stigmatisation se pose avec acuité. Bien que les systèmes de surveillance ne soient pas mis en place dans le but de créer de la discrimination et de la stigmatisation, la Commission considère qu'il s'agit d'un détournement d'usage aussi vraisemblable qu'inacceptable.

Malgré tout, les NTSC offrent un potentiel très intéressant en matière de surveillance, ainsi que pour l'évaluation et la gestion des risques sur le plan de la sécurité. Ce point ne doit être ni négligé ni sous-estimé. Si d'aucuns voient dans la popularité croissante des moyens de surveillance une menace pour les droits et libertés des citoyens dans une société démocratique, les plus optimistes feront valoir que ces mêmes moyens peuvent contribuer à la prévention de la criminalité, voire du terrorisme.

Bien qu'ils puissent servir la prévention du crime, les détournements d'usage posent des risques de dérives et d'abus qui commandent une grande attention. En donnant l'aval à l'exploitation de toutes les utilisations possibles des NTSC afin de protéger la démocratie et l'ordre public contre le terrorisme et les autres formes de criminalité, la Commission craint justement le sacrifice de droits et de libertés qui fondent la démocratie. La Commission insiste tout au long du présent avis sur la nécessité de trouver des équilibres et elle en vient à la conclusion que la démocratie elle-même constitue un équilibre toujours fragile entre la liberté et la répression. Elle estime que les NTSC peuvent faire beaucoup pour améliorer la sécurité du public, mais croit par ailleurs qu'il n'est pas toujours nécessaire d'exploiter toutes les utilisations possibles qui leur sont associées pour assurer un niveau acceptable de sécurité.

La protection des renseignements personnels

La question des NTSC est souvent ramenée à un seul enjeu : la protection des renseignements personnels. Cette importance est notamment due au fait que les NTSC sont principalement déployées pour recueillir des renseignements (qui sont souvent personnels). Cet enjeu, plus que tout autre, concerne les valeurs de respect de la vie privée et de sécurité. Si, d'un côté, les renseignements personnels en disent long sur la vie privée des personnes, ils sont souvent vus comme une source riche d'informations permettant d'améliorer la sécurité.

La protection des renseignements personnels est presque systématiquement associée au respect de la vie privée. Il est vrai que les renseignements dits personnels ouvrent une fenêtre sur divers aspects de notre vie privée. En fait, la protection des renseignements personnels constitue un moyen d'actualiser la valeur de la vie privée. Si la première est davantage un concept juridique, le respect de la vie privée, dans le cadre du présent avis, doit être entendu comme une valeur.

Les données recueillies par des systèmes biométriques, par la vidéosurveillance et par l'IRF sont presque systématiquement des renseignements personnels. Par conséquent, le niveau de respect de la vie privée des personnes objets de la surveillance variera en fonction de l'utilisation, de la communication et de la conservation qui seront faites de ces données.

La protection des renseignements personnels est indissociable des systèmes biométriques, car les mesures biométriques sont considérées comme des renseignements personnels. Le fait que certaines données biométriques constituent des identifiants intimes bavards explique probablement pourquoi les systèmes biométriques font parfois craindre le pire en ce qui a trait au respect de la vie privée des personnes. Les données biométriques peuvent être qualifiées d'identifiants intimes, du fait qu'elles sont étroitement liées à l'individu auquel elles se rapportent. Le caractère bavard de certains identifiants biométriques constitue également un objet d'inquiétude :

les données biométriques portent en elles-mêmes plus d'informations que la simple reproduction de l'image d'une empreinte digitale, par exemple. En effet, selon certains experts, il est même possible de récolter des informations sur l'état de santé ou encore sur l'humeur des individus seulement par l'analyse des empreintes digitales ou encore de la rétine. Les personnes préfèrent généralement que certaines informations qui sont en leur possession et qui les concernent personnellement demeurent confidentielles ou, du moins, qu'elles soient traitées comme telles.

Par son caractère invisible et distant, la vidéosurveillance peut représenter une menace pour la vie privée. En effet, la technologie permet de filmer des personnes à leur insu, tant dans des lieux publics que dans des endroits privés. Or, en circulant dans des lieux publics, une personne doit admettre qu'elle ne bénéficie pas de la même intimité que dans sa maison, par exemple. Toutefois, ce serait abuser de ce principe que de prétendre que la personne renonce totalement au respect de sa vie privée dans les lieux publics. Toute personne est aussi en droit de circuler dans des lieux publics sans être constamment l'objet d'une surveillance. Le respect de la vie privée s'applique même dans des lieux publics.

Tout comme la vidéosurveillance, l'identification par radiofréquence (IRF) peut s'avérer une méthode subreptice de surveillance et être utilisée pour suivre des personnes à la trace. C'est pourquoi les commentaires de la Commission au sujet de la vidéosurveillance s'appliquent aussi dans le cas de l'IRF. Cependant, la Commission désire attirer l'attention sur le fait que la nature des renseignements personnels recueillis est différente. Dans le cas de la vidéosurveillance, ce sont les images captées et donc possiblement le visage des personnes qui seront les renseignements personnels. Pour l'IRF, des renseignements personnels cruciaux sont susceptibles d'être recueillis et utilisés : informations sur le crédit, la santé, l'identité, la nationalité, etc. La nature de ces renseignements pose donc des risques accrus d'atteinte à la vie privée des citoyens.

Considérant que les nouveaux passeports des citoyens de la plupart des membres de l'Union européenne et ceux maintenant délivrés aux citoyens américains comportent une puce d'IRF et devant l'intérêt déjà manifesté par le gouvernement du Canada pour l'introduction de données biométriques dans les documents d'identité des citoyens canadiens, la Commission estime qu'il faut rapidement statuer sur la manière d'encadrer l'introduction de ces technologies dans les documents d'identité. En outre, les expériences européenne et américaine montrent l'importance de protéger les renseignements personnels de manière adéquate si l'objectif de sécurisation des documents d'identité doit être atteint. Pour sa part, et considérant les risques élevés en matière de respect de la vie privée et de protection des renseignements personnels, la Commission estime important que le gouvernement du Québec travaille de concert avec les instances concernées au sein du gouvernement du Canada pour que, dans l'éventualité d'une introduction de puces d'IRF dans les documents d'identité des Canadiens, ces puces d'IRF contenant des renseignements personnels soient dotées d'un procédé de chiffrement qui permette de sécuriser les données et, ainsi, de mieux protéger la vie privée et d'assurer une meilleure protection des renseignements personnels.

Il serait inacceptable que des décisions basées sur des traitements automatisés deviennent monnaie courante dans le milieu de la surveillance et du contrôle de l'identité. La déshumanisation complète de la décision sécuritaire doit être évitée. Ici encore, il semble qu'un équilibre doit être atteint entre la part dévolue aux personnes et celle confiée à la machine en ce qui a trait à la surveillance et aux traitements des données recueillies. D'un côté, plus la part de gestion et d'administration des systèmes de surveillance est l'affaire de personnes, plus il faut s'attendre à ce que les expériences de vie de ces gestionnaires influent parfois sur leurs décisions. Mais il est inutile de se leurrer : personne n'est en mesure de faire totalement abstraction de ses opinions personnelles dans la conduite de son travail. D'autre part, si le traitement automatisé et informatisé des données peut réduire la part de l'influence des opinions et des préjugés des opérateurs de systèmes de surveillance, il n'en demeure pas moins inquiétant de savoir que des décisions préjudiciables peuvent être prises sur la base de ce traitement sans que qui que ce soit ait pu remettre en contexte les informations traitées.

Enfin, il faut se demander si le niveau de protection des renseignements personnels est le même d'un pays à l'autre et si le transfert de ces renseignements d'un pays doté de mesures favorisant largement la protection des données personnelles vers un pays qui n'a pas autant à offrir est acceptable. Déjà, les consommateurs traitent sur Internet

avec des entreprises de l'extérieur du pays qui conservent des renseignements personnels à leur égard, sans qu'ils connaissent toujours la manière dont ces renseignements seront protégés. Or, dans ces cas, les consommateurs sont toujours libres de ne pas effectuer ce genre de transactions. Mais en ce qui concerne des renseignements obtenus par le moyen de NTSC, les personnes ne savent pas toujours que des renseignements personnels les concernant seront conservés. Manifestement, une telle perspective n'est pas sans poser la question du contrôle de l'individu sur la direction que peuvent prendre ses renseignements personnels.

Le présent avis met en lumière des questions auxquelles la Commission n'est pas en mesure de répondre et dont elle ne peut assurer le suivi. Toutefois, celle-ci estime que plusieurs actions doivent être entreprises pour apporter des solutions et que les acteurs gouvernementaux en mesure de les accomplir sont facilement identifiables.

Considérant que le ministre responsable des Affaires intergouvernementales canadiennes, des Affaires autochtones, de la Francophonie canadienne, de la Réforme des institutions démocratiques et de l'Accès à l'information a pour mandat de conseiller le gouvernement en lui fournissant des avis en matière d'accès à l'information et de protection des renseignements personnels, notamment lors de la présentation de projets de loi ou du développement de systèmes d'information et qu'à cette fin il peut consulter la Commission d'accès à l'information ;

Considérant que la Commission d'accès à l'information est chargée d'assurer le respect et la promotion de l'accès aux documents et de la protection des renseignements personnels et qu'elle peut prescrire des conditions applicables à un fichier de renseignements personnels auxquelles l'organisme public doit se conformer ;

Considérant que la Commission d'accès à l'information peut également, au terme d'une enquête relative à la collecte, à la détention, à la communication ou à l'utilisation de renseignements personnels par une personne qui exploite une entreprise, après lui avoir fourni l'occasion de présenter ses observations, lui recommander ou lui ordonner l'application de toute mesure corrective propre à assurer la protection des renseignements personnels ;

Et considérant que la Commission des droits de la personne et des droits de la jeunesse du Québec a notamment pour mandats :

- *d'élaborer et d'appliquer un programme d'information et d'éducation, tant en matière de droits de la personne que de protection des droits de la jeunesse ;*
- *de diriger et encourager les recherches et les publications sur les libertés et droits fondamentaux et sur les droits de la jeunesse ;*
- *de recevoir les suggestions, recommandations et demandes touchant les droits et libertés de la personne, en tenant des auditions publiques au besoin, et d'adresser au gouvernement les recommandations appropriées ;*
- *de coopérer avec toute organisation vouée à la promotion des droits et libertés de la personne, au Québec ou à l'extérieur,*

la Commission recommande au ministre responsable des Affaires intergouvernementales canadiennes, des Affaires autochtones, de la Francophonie canadienne, de la Réforme des institutions démocratiques et de l'Accès à l'information, à la Commission d'accès à l'information et à la Commission des droits de la personne et des droits de la jeunesse du Québec de collaborer ensemble dans le but de mettre en œuvre les actions suivantes :

1. Favoriser le dialogue entre les citoyens, le gouvernement et l'industrie en vue d'adopter des lignes directrices pour l'utilisation de ces technologies qui tiennent compte des préoccupations éthiques en la matière et des valeurs fondamentales des sociétés démocratiques.
2. Suivant une approche consultative, conseiller le gouvernement dans ses projets de déploiement de NTSC, notamment sur les aspects soulevant des enjeux éthiques et à la lumière des critères de pertinence, d'efficacité et de fiabilité.
3. Organiser une consultation de la population (sur le modèle du forum citoyen tel qu'élaboré par le Commissaire à la santé et au bien-être) qui ferait une place importante aux enjeux éthiques.
4. Diffuser les résultats de cette consultation dans la population afin de la sensibiliser aux questions d'éthique associées aux NTSC.
5. Informer la population quant aux dispositions juridiques entourant le déploiement des NTSC, à ses conséquences pour les valeurs d'autonomie, de liberté, de sécurité et de vie privée et aux moyens mis à la disposition des citoyens pour participer à la prise de décision, à la mise en œuvre et au suivi en la matière.
6. Mettre en place un mécanisme de réparation et de rectification pour les cas où l'utilisation des NTSC cause des préjudices à des personnes en les associant à tort à des activités illicites.

Introduction

À sa réunion du 9 décembre 2003, la Commission de l'éthique de la science et de la technologie a retenu la biométrie comme thème de réflexion pour la production d'un avis. À cette fin, et dans un premier temps, elle a produit un document de réflexion et un document de consultation qui ont servi de fondement à la tenue d'un forum public sur les enjeux soulevés par l'utilisation des données biométriques qui s'est tenu en octobre 2004. Le forum a été organisé conjointement avec la Chaire Raoul-Dandurand en études stratégiques et diplomatiques de l'Université du Québec à Montréal. Le document de consultation a également servi à la mise en place d'une consultation en ligne qui invitait la population ou tout organisme intéressé à soumettre des commentaires ou un mémoire en vue d'enrichir la réflexion de la Commission.

Toutefois, et à la suite des travaux réalisés sur l'utilisation des données biométriques, la Commission s'est donné le mandat de formuler un avis non seulement sur ce sujet, mais aussi sur d'autres technologies pouvant servir à la surveillance de masse à des fins de sécurité : la vidéosurveillance et l'identification par radiofréquence (IRF). À la suite des travaux réalisés pour la publication de son avis sur les nanotechnologies, il lui semblait important d'élargir le thème de la biométrie afin d'y intégrer de nouvelles technologies de surveillance et de contrôle (NTSC) qui, tout en ne reposant pas nécessairement sur l'utilisation de données biométriques, sont de plus en plus utilisées à des fins de sécurité.

Certaines technologies ont dû être mises de côté, soit parce qu'elles méritaient un traitement à part entière en raison de leur complexité et de leur manière d'utiliser des données (cybersurveillance et forage des données), soit parce qu'elles ne s'appliquaient qu'à la surveillance de certaines personnes (bracelets servant à la géolocalisation). En outre, la Commission a choisi de traiter des NTSC sous l'angle de leurs applications à des fins de sécurité, ce qui excluait notamment les fins de surveillance sur les lieux de travail, les fins associées à la santé et les applications liées à la gestion des inventaires.

La mission de la Commission consiste, entre autres, à proposer des orientations susceptibles de guider les acteurs concernés dans leur prise de décision. Dans le présent avis, les acteurs visés étant institutionnels, il est davantage question de la surveillance effectuée par l'État sur les citoyens que de la surveillance exercée par les citoyens sur d'autres citoyens ou sur l'État. Cependant, lorsqu'il lui apparaît pertinent de le faire, la Commission se penche également sur cette dimension de la surveillance.

Le déploiement des NTSC est intimement lié au contexte social, sociopolitique, éthique et juridique de l'époque actuelle. Le premier chapitre tente de brosser le tableau de ce contexte en attirant l'attention du lecteur sur différents éléments. Tout d'abord, la Commission précise ce qu'elle entend par l'expression « à des fins de sécurité » et ce que celle-ci inclut. De plus, elle traite du sentiment d'insécurité auquel il est souvent fait référence dans les médias. Il s'avère en fait que le sentiment que les gens ont de leur propre sécurité dépend de plusieurs facteurs et qu'il peut être influencé par différents acteurs. Pour tenter de mieux évaluer l'ampleur réelle du sentiment d'insécurité, la Commission a examiné plusieurs enquêtes et sondages sur le sujet.

Ensuite, considérant que le déploiement des NTSC est étroitement associé au contexte sociopolitique de l'époque moderne, la Commission attire l'attention sur la place de plus en plus grande accordée à l'évaluation, à la gestion et à l'élimination des risques. Plusieurs penseurs estiment que le fait d'être obsédé par les risques, les menaces et les dangers est un symptôme de l'insécurité qui affecte une société. C'est d'ailleurs pourquoi des auteurs, comme le sociologue Ulrich Beck, qualifient ces sociétés de sociétés du risque.

Les NTSC sont de plus en plus présentes dans le quotidien des citoyens des sociétés modernes. À tel point qu'à l'instar de quelques observateurs la Commission émet l'hypothèse selon laquelle l'expression « sociétés de surveillance » sera applicable à la plupart des sociétés modernes dans un avenir rapproché.

D'entrée de jeu, la Commission définit le cadre éthique dans lequel elle inscrit sa réflexion pour porter un regard éthique sur les NTSC. Elle précise les valeurs en jeu et esquisse les enjeux éthiques qui feront l'objet d'un développement au troisième chapitre. À l'égard des valeurs, la Commission souligne son attachement à plusieurs valeurs fondamentales au sein des sociétés démocratiques. L'objectif à atteindre selon elle est un juste équilibre entre la sécurité et les droits et libertés individuels dans la protection des valeurs fondamentales des sociétés démocratiques.

Les principaux textes normatifs qui balisent et réglementent déjà cette pratique sont également signalés. Un rapide survol est fait des instruments normatifs en vigueur à l'échelle québécoise, canadienne, régionale et internationale.

Le deuxième chapitre contient une description relativement détaillée des trois NTSC sur le plan technique : les systèmes biométriques, la vidéosurveillance et l'identification par radiofréquence (IRF). Un système biométrique permet d'identifier une personne ou vérifie l'admissibilité d'une personne « à se voir reconnaître certains droits ou services (notamment l'accès) basés sur la reconnaissance de particularités physiques (empreintes digitales, iris de l'œil, contour de la main...), de traces (ADN, sang, odeurs) ou d'éléments comportementaux (signature, démarche)[1] ». Les applications des systèmes biométriques sont encore plutôt rares. La vidéosurveillance, par contre, est une technologie de surveillance beaucoup plus répandue et familière. Il est toutefois moins certain que les plus récentes avancées technologiques en la matière (comme la numérisation, le couplage avec des logiciels de reconnaissance faciale, par exemple) soient aussi connues. Enfin, l'identification par radiofréquence, sans être véritablement une nouvelle technologie, trouve actuellement des applications surprenantes, et cela, dans divers domaines. En matière de sécurité, l'insertion de puces contenant des renseignements personnels ou d'autres informations (la nationalité, le sexe, la date de naissance, etc.) dans les documents d'identité et les cartes d'accès est la principale application de l'IRF. Pouvant être lues à distance, ces puces permettraient de suivre des personnes à la trace et de sécuriser des documents afin d'éviter la fraude et le vol d'identité.

La Commission pose un regard proprement éthique sur les NTSC et leurs applications dans le troisième chapitre. Tour à tour, les principaux enjeux éthiques et les valeurs privilégiées sont mis en perspective : l'évaluation de la pertinence, de l'efficacité et de la fiabilité des NTSC, la proportionnalité de la réponse à l'insécurité, l'acceptabilité sociale, le consentement, le respect des finalités, la protection des renseignements personnels.

Avec cet avis, la Commission souhaite contribuer à faire avancer la réflexion éthique sur le déploiement des NTSC, mais aussi fournir aux principaux acteurs des orientations qui prennent en considération les enjeux éthiques et les valeurs fondamentales au sein des sociétés démocratiques. S'inscrivant dans un débat où les protagonistes ont souvent des opinions très tranchées, le présent avis propose un discours qui se veut le plus objectif et le plus nuancé possible. Ce n'est pas en agitant le spectre du retour imminent des sociétés totalitaires ni en adoptant un point de vue complaisant sur les nouvelles applications des NTSC que l'État québécois arrivera à prendre toute la mesure des changements qui s'opèrent déjà et qui continueront de s'opérer en la matière. Une attitude qui vise un juste équilibre entre la prudence et l'audace, entre la méfiance et la naïveté et qui privilégie la concertation des principaux acteurs, la consultation et la sensibilisation de la population, de même qu'un encadrement éthique approprié, est par conséquent de mise.

1. Définition de la Commission nationale de l'informatique et des libertés (CNIL – France), rapportée dans OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, *Les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre*, Rapport présenté au Sénat par Christian CABAL, Assemblée nationale (France), juin 2003, note 6, p. 8.

Chapitre 1
Le déploiement des nouvelles technologies de surveillance et de contrôle à des fins de sécurité : un phénomène en continuité avec la modernité[2]

Pourquoi le déploiement des nouvelles technologies de surveillance et de contrôle (NTSC) connaît-il un essor aussi fulgurant aujourd'hui ? Pour répondre à cette question, il faut mettre en perspective le contexte qui stimule la demande pour de telles technologies. Ce contexte se caractérise notamment par une volonté de renforcer la sécurité. Or, un plus grand attachement à la sécurité se fait possiblement l'écho d'un sentiment d'insécurité. Pour tenter d'y voir plus clair, la Commission prend la notion de sentiment d'insécurité pour point de départ d'un parcours qui l'amène à se pencher sur d'autres éléments contextuels : la place de plus en plus grande que prennent le risque et la surveillance dans la société. De plus, la Commission donne un aperçu des valeurs et des enjeux éthiques qui retiennent son attention au sujet du déploiement des NTSC à des fins de sécurité. Ce survol est complété par une présentation de l'encadrement normatif en la matière.

La sécurité : une notion à préciser

Qu'est-ce que la sécurité ? Poser la question met en évidence la complexité du concept. En effet, non seulement le terme renvoie à différentes notions, notamment sur le plan sociologique, mais son interprétation varie en fonction des langues, des discours, des approches et de l'histoire. Quatre questions clés jalonnent le débat sur la notion de sécurité[3] : « Quelle est la nature de l'insécurité ? » ; « À quel objet la sécurité fait-elle référence ? » ; « Qui en assume la responsabilité ? » ; « Quels sont les moyens d'assurer la sécurité ? ».

La sécurité comporte deux dimensions[4] : 1) l'une, objective, qui fait intervenir des paramètres permettant, en quelque sorte, de mesurer le degré de sécurité réel ou l'absence de menaces et de dangers ; 2) l'autre, subjective, qui renvoie davantage au sentiment que les personnes éprouvent par rapport à leur sécurité. Ces deux dimensions s'influencent réciproquement.

Assurer la sécurité d'un territoire, d'un pays, d'une ville, d'une habitation est un défi constant, car il faut, d'une part, déterminer correctement les menaces et, d'autre part, mettre en place un système efficace de protection. À l'heure actuelle, surtout depuis les événements du 11 septembre 2001, les paramètres du danger et de la sécurité semblent entièrement nouveaux et paraissent exiger l'adoption de mesures également nouvelles, sur le plan tant technique que politique. Bien que ces événements aient rappelé que nos sociétés ne sont jamais totalement en sécurité, ils ont surtout eu un impact sur le sentiment d'insécurité de la population. L'implantation des NTSC constitue possiblement un élément de ce qu'il est convenu d'appeler la théâtralisation de la sécurité, soit un moyen de rassurer les citoyens quant à leur sécurité.

2. Le terme « modernité » est ici entendu dans son sens philosophique. En outre, cette notion peut à la fois désigner le courant philosophique et une période de l'histoire de la philosophie, caractérisée par la prédominance de ce courant. Le *Grand Dictionnaire de la philosophie* de Larousse donne la définition suivante : « Caractère propre de ce qui passe pour moderne, s'affirmant moins par la rupture d'avec le passé que par l'orientation vers l'avenir : la modernité vit dans le présent le choc du futur, elle pressent ce qui sera tout autant qu'elle dénonce ce qui n'est plus. Aussi faut-il la distinguer de l'actualité, qui se borne au constat de l'aujourd'hui, sans souci de prophétie. »

3. Isabelle MASSON, « Sécurité », dans Alex MACLEOD, Evelyne DUFAULT et F. Guillaume DUFOUR (dir.), *Relations internationales : théories et concepts*, Montréal, Athéna éditions, 2004, p. 216.

4. ORGANISATION MONDIALE DE LA SANTÉ, *Sécurité et promotion de la sécurité : aspects conceptuels et opérationnels*, septembre 1998, p. 8 et 9.

Le sentiment d'insécurité : une réalité difficile à cerner

Le sentiment d'insécurité demeure une notion nébuleuse. Tout comme pour le concept de sécurité, il est important de distinguer l'insécurité du *sentiment* d'insécurité. L'insécurité est un « manque de sécurité », une « situation où l'on est menacé, exposé aux dangers[5] », alors que le sentiment d'insécurité est un état émotif résultant de l'évaluation subjective des dangers. Ce sentiment varie d'une personne à l'autre selon le degré de confiance en soi, par exemple.

Dans le cadre du présent avis, c'est la notion de *sentiment* d'insécurité qui retient l'attention de la Commission. Bien que les décisions sécuritaires des organisations publiques et privées puissent être motivées par une menace réelle, le plus souvent les mesures prises se fondent sur la perception de cette menace. À ce propos, le déploiement des NTSC n'empêchera pas systématiquement des crimes de se commettre, mais il contribuera à rassurer la population.

Une distinction importante mérite d'être faite en ce qui concerne le sentiment d'insécurité. En premier lieu, il faut dissocier la préoccupation sécuritaire ou peur diffuse, soit « une inquiétude diffuse à l'égard du crime en tant que phénomène de société, souvent associée à des opinions favorables au durcissement de l'appareil répressif[6] », et la peur du crime proprement dit ou peur concrète, qui revient à une « appréhension personnelle déclarée par l'individu dans un contexte spécifique ». Ces deux sentiments ne vont pas nécessairement de pair : une personne peut très bien juger que l'insécurité est un problème grave sans pour autant se sentir personnellement en danger, et inversement. De plus, ces deux niveaux du sentiment d'insécurité entraînent des réactions différentes, des besoins différents et se caractérisent par des origines différentes[7]. Ainsi, la peur diffuse s'enracine dans des idées et des préjugés entretenus au sujet de la criminalité, des criminels et de la justice en général, alors que la peur concrète doit être analysée selon le contexte de vie précis de personnes ciblées. De manière générale, il est possible d'affirmer que la peur diffuse est plus répandue que la peur concrète[8].

Il existe de nombreuses causes au sentiment d'insécurité, et leur importance varie d'une personne à l'autre. C'est pourquoi il serait utopique de tenter d'en dresser un inventaire exhaustif.

Le rôle des médias

Les médias laissent entendre que le crime est partout. L'importante couverture médiatique accordée à la criminalité et aux événements extraordinaires (catastrophes naturelles, attentats terroristes, guerres, etc.) suscite des peurs hors de proportion avec les statistiques sur le sujet[9]. Par le traitement que les médias font de certains événements, ils enrichissent l'imaginaire collectif et influencent l'appréhension que la population peut avoir de divers dangers[10]. Ainsi, sera plus redouté un danger grave mais rare, par exemple un attentat terroriste, qu'un danger plus concret lié à la vie quotidienne, tel un accident de voiture. En outre, la couverture médiatique des statistiques concernant la criminalité et celle des faits divers concernant des actes criminels sont disproportionnées : « Alors que la nouvelle portant sur la diminution de la criminalité n'aura qu'un faible écho une fois l'an lors de la parution des statistiques, les histoires criminelles seront couvertes quotidiennement par les médias[11]. »

5. « Insécurité », dans *Le Petit Robert*, édition de 1993, p. 1182.
6. Patrick PERETTI-WATEL, *Sociologie du risque*, Paris, Armand-Colin, 2000, p. 162.
7. MINISTÈRE DE LA SÉCURITÉ PUBLIQUE DU QUÉBEC, *Pour un Québec plus sécuritaire : partenaires en prévention*, Rapport de la Table ronde sur la prévention de la criminalité, 1993, [http://www.msp.gouv.qc.ca/prevention/prevention.asp?txtSection=publicat&txtCategorie=table_ronde].
8. MINISTÈRE DE LA SÉCURITÉ PUBLIQUE DU QUÉBEC, *op. cit.*
9. David LE BRETON, *Sociologie du risque*, Paris, Presses Universitaires de France, 1995, p. 35.
10. *Ibid.*
11. Olivier LAMALICE, *Opinions publiques, incarcération et système pénal aux États-Unis : les influences de la classe politique et des médias*, document d'appoint préparé pour le ministère de la Sécurité publique, p. 26, [http://www.msp.gouv.qc.ca/reinsertion/reinsertion.asp?txtSection=publicat].

Si l'influence des médias semble si grande, c'est que la perception des dangers constitue un facteur clé dans le sentiment d'insécurité de la population. Or, les médias ont un impact sur cette perception, comme le montre une enquête du ministère de la Sécurité publique[12] et la plus récente enquête de Statistique Canada sur la victimisation[13]. Il suffit de penser au nombre grandissant de chaînes spécialisées en information continue et à leur popularité pour prendre conscience de l'importance sociale accordée aux médias d'information et à leur message.

Le rôle politique de la peur du crime

En plus des médias, divers acteurs alimentent également le sentiment d'insécurité, dont les élites politiques et des groupes d'intérêts[14]. Dans un document préparé pour le ministère de la Sécurité publique se trouve un exemple éloquent :

> *La perception, souvent erronée, de la situation du crime aux États-Unis par la population a été influencée par une couverture grandissante des actes criminels, par une généralisation de la violence dans les ghettos et par une capitalisation politique de l'insécurité créée par une telle couverture journalistique. En effet, alors que le nombre de reportages portant sur la criminalité double entre 1992 et 1993 et que la criminalité diminue généralement depuis 1980, le président Clinton présentait en 1993 au Congrès une sévère loi de guerre à la criminalité, profitant du climat politique favorable*[15].

La peur du crime joue un rôle politique indéniable, si bien qu'elle peut être considérée comme un objet de gouvernance[16]. D'abord, la peur du crime est l'objet de stratégies qui visent à la réduire ou à la contenir, l'objectif étant de rassurer la population. Mais elle peut aussi être brandie dans le but d'encourager les individus à adopter des comportements et des habitudes de vie qui réduisent leur exposition au risque d'être victimes d'un crime. Bref, afin de motiver les individus à rester prudents, il faut trouver un juste milieu entre la réduction de la peur du crime qui effraie et qui paralyse l'action et le rappel des dangers liés à la criminalité.

Le rappel des dangers liés à la criminalité se situe dans le sillage d'une philosophie de la peur en général. D'Alexis de Tocqueville à Hannah Arendt, plusieurs penseurs de la philosophie occidentale considèrent la peur comme un instrument permettant de galvaniser l'action et qui concourt à la préservation des libertés durement acquises[17]. Selon ce courant de pensée, la peur du retour des goulags et des camps de concentration, pour donner des exemples récents, encouragerait les sociétés à tout faire pour éviter que de telles atrocités ne se répètent. Dans le domaine de l'environnement, le philosophe Hans Jonas a renouvelé cette pensée de la peur comme guide de l'action prudente et responsable à travers le concept d'heuristique de la peur[18]. Selon lui, le développement des sciences et de la technologie offre aujourd'hui à l'humanité, et pour la première fois, la possibilité de s'autodétruire. Les catastrophes passées et appréhendées suscitent par conséquent une peur qui peut servir de guide à l'humanité dans sa recherche pour des actions responsables et qui ne compromettent pas les conditions d'existence de la vie humaine aujourd'hui et pour les générations futures.

Quelle est l'ampleur du sentiment d'insécurité et que craint-on ?

Il importe de savoir si, dans les faits, il existe bel et bien un sentiment d'insécurité et, si oui, quels sont les objets de ces craintes. La Commission a donc procédé à une analyse de quelques sondages et enquêtes sur le sujet.

Le sentiment d'insécurité constitue une réalité difficilement quantifiable, et les questions posées dans les sondages et les enquêtes sont souvent trop peu précises. La plupart du temps, ces questions cherchent à savoir si

12. MINISTÈRE DE LA SÉCURITÉ PUBLIQUE DU QUÉBEC, *op. cit.*
13. STATISTIQUE CANADA, *Enquête sociale générale sur la victimisation, cycle 18 : un aperçu des résultats*, Ottawa, Canada, 2004, p. 7. [http://dsp-psd.pwgsc.gc.ca/Collection/Statcan/85-565-X/85-565-XIE.html].
14. Corey ROBIN, *Fear. The History of a Political Idea*, New York, Oxford University Press, 2004, p. 16.
15. Olivier LAMALICE, *op. cit.*, p. 2.
16. Murray LEE, « Governing 'Fear of Crime' », dans *Hard Lessons*, Richard Hil et Gordon Tait (dir.), Ashgate, Hants, 2004, p. 35.
17. Corey ROBIN, *op. cit.*, p. 9-10.
18. Voir Hans JONAS, *Le principe responsabilité : une éthique pour la civilisation technologique*, Paris, Éditions du Cerf, 1990.

les gens se sentent en sécurité à la maison, s'ils ont peur de marcher seuls dans les rues le jour, la nuit. À ce sujet, les sondages sont sans équivoque. Selon un sondage Léger Marketing[19] de janvier 2003, la quasi-totalité des Canadiens se sent en sécurité à la maison (97 %). De plus, 84 % des Canadiens n'ont pas peur de sortir seuls le soir ou la nuit. Un sondage[20] portant sur le sentiment de sécurité des Montréalais est lui aussi révélateur : 90 % d'entre eux se sentent en sécurité dans la métropole et 73 % estiment que le transport en commun à Montréal est sécuritaire. En 2007, un sondage[21] révélait que, selon 70 % des répondants, Montréal est une ville sécuritaire. Enfin, l'enquête sociale générale menée par Statistique Canada en 2004 révèle que les Canadiens se sentent de plus en plus en sécurité, ce qui va à l'encontre de la tendance remarquée il y a une quinzaine d'années :

> *Le sentiment de satisfaction à l'égard de la sécurité personnelle chez les Canadiens âgés de 15 ans et plus s'accroît depuis 1993, pour s'établir à 94 %. Lorsqu'on leur demande d'évaluer ce sentiment dans diverses situations, le pourcentage demeure élevé, quoique légèrement inférieur. En effet, quatre personnes sur cinq (80 %) disent ne pas avoir d'inquiétude lorsqu'elles sont seules à la maison le soir.* [...]
>
> *Selon les résultats de l'ESG de 2004, près de six Canadiens sur dix (58 %) pensent que le taux de criminalité dans leur voisinage n'a pas changé depuis cinq ans. Un autre 30 % de la population pense que la criminalité s'est aggravée dans leur voisinage, tandis que 6 % exprime l'avis que la criminalité a diminué. En général, les opinions se sont améliorées depuis 1993 alors que les Canadiens étaient plus enclins à dire que la criminalité dans leur voisinage était en hausse (46 %) plutôt que stable au cours des cinq années précédentes (43 %).* [...]
>
> *En 2004, la très grande majorité des Canadiens pensaient qu'ils ne couraient pas de risque d'être victimes et cette proportion est en croissance. En effet, 94 % des Canadiens pensent être assez ou très protégés contre le crime, comparativement à 91 % en 1999 et à 86 % en 1993*[22].

Plusieurs sondages s'intéressent à la menace terroriste. Celle-ci revêt souvent un aspect plus spectaculaire que la criminalité dite traditionnelle. Comme l'un des objectifs des terroristes est d'instaurer un climat de peur et d'insécurité, ceux-ci ont recours à des méthodes qui, sans être toujours nouvelles, cherchent à surprendre[23]. Par conséquent, il se peut qu'un citoyen se dise à l'abri des dangers associés à la criminalité « traditionnelle », alors qu'il ne se considère pas comme étant à l'abri d'un attentat terroriste, et ce, bien que les probabilités d'être victime d'un crime soient beaucoup plus grandes que celles d'être victime d'un attentat terroriste, du moins au Canada.

Cela dit, la population québécoise et canadienne se sent-elle menacée par le terrorisme ? Que nous révèlent à ce sujet les sondages d'opinion et les enquêtes publiées au Canada ? Depuis les événements de septembre 2001, la firme canadienne Compas mène annuellement un sondage auprès de gens d'affaires du pays[24]. Dans le cadre de ce sondage, il est systématiquement question du sentiment de sécurité chez les répondants. En novembre 2001, à la question : « Selon vous, quelle est la probabilité qu'une attaque terroriste de la magnitude de celle du 11 septembre 2001 contre le World Trade Center se produise [au Canada] dans les douze prochains mois ? », les gens d'affaires ont répondu que cette probabilité s'élevait à 20 %. Cette probabilité descend à 12 % et à 15 % respectivement en 2002 et en 2003. Puis, par deux fois, et chaque fois à la suite d'autres attentats terroristes, cette probabilité augmente. En août 2004 (attentats de Madrid en mars de la même année), la probabilité grimpe à 23 % et, en juillet 2005 (attentats de Londres ce même mois), elle se hisse à 24 %. L'inconvénient majeur d'une telle question tient à son caractère incomplet. La réponse donne l'estimation que les gens font de la probabilité qu'il y ait un attentat terroriste et non pas qu'ils se sentent en sécurité ou non sachant qu'il peut y en avoir un.

19. LÉGER MARKETING, *Le sentiment de sécurité des Canadiens*, janvier 2003.
20. LÉGER MARKETING, *Étude sur le sentiment de sécurité des Montréalais*, mars 2004.
21. LÉGER MARKETING, *Montréal une ville sécuritaire, attrayante mais malpropre*, février 2007.
22. STATISTIQUE CANADA, *op. cit.*, p. 8-9.
23. Pour une définition complète du terrorisme, voir le document de réflexion de la Commission intitulé *L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques*, Sainte-Foy, 2005, p. 16-17.
24. COMPAS, *Terror after London*, BDO Dunwoody/Chamber Weekly CEO/Business Leader Poll by Compas in the Financial Post, 18 juillet 2005, p. 5.

Fait intéressant, lorsque les sondeurs demandent quelle est la principale raison pour laquelle le Canada serait une cible éventuelle, les répondants pensent, dans une proportion de 45 %, que la médiocrité des contrôles frontaliers et de la sécurité au Canada constitue la principale raison. Un sondage de la firme Léger Marketing[25] réalisé en 2002 indique que la très grande majorité (94 %) des Canadiens estime que le Canada est un pays sécuritaire. Néanmoins, 82 % des Canadiens voudraient que le gouvernement investisse autant ou plus d'argent pour la sécurité du pays. En outre, 56 % des Canadiens estiment qu'il serait facile ou très facile pour un réseau de terroristes de déjouer les systèmes de sécurité canadiens. Dans un sondage de février 2003 mené par la firme EKOS, les répondants estiment que la meilleure solution à long terme afin de protéger le Canada du terrorisme est une augmentation des dépenses en matière de sécurité et de services des renseignements.

Toujours en ce sens, un autre sondage, cette fois mené par la firme Strategic Counsel[26] et datant d'août 2005, révèle que 62 % des répondants croient qu'une attaque terroriste se produira au Canada dans les prochaines années. De plus, seulement 25 % d'entre eux disent que le Canada est bien préparé à faire face à un attentat terroriste. Un an plus tard, le même sondage donne des résultats légèrement différents[27]. Si c'est alors 71 % des répondants qui estiment probable qu'un acte terroriste sera perpétré au Canada dans les prochaines années, 37 % (au lieu de 25 %) considèrent que le Canada est prêt à gérer la menace terroriste. Reste tout de même que 56 % d'entre eux pensent le contraire. Lorsque la question de l'imminence d'une attaque terroriste est posée, la proportion des répondants qui pensent que le Canada sera pris pour cible par des attaques terroristes à court terme chute à 37 %[28].

Les sondages révèlent en outre que les Canadiens semblent très peu préoccupés par les menaces que font peser sur leurs droits les mesures pour combattre le terroriste[29]. À la question : « Le débat sur la guerre au terrorisme a-t-il été trop orienté vers les mesures pour combattre le terrorisme ou vers la protection des libertés civiles ? », 13 % des personnes sondées ont répondu qu'un trop grand accent avait été mis sur les mesures pour combattre le terrorisme, alors que 26 % pensaient que le débat était trop orienté vers la question de la protection des libertés civiles. Enfin, 46 % des répondants étaient d'avis que le débat avait atteint un juste équilibre entre ces deux tendances. Aux États-Unis, selon un sondage mené en 2006, 68 % des Américains croient qu'ils devront abandonner une partie de leurs libertés individuelles afin de sécuriser leur pays contre le terrorisme. Le sentiment de sécurité des Américains a été évalué récemment par la voie d'un sondage d'une grande ampleur[30]. Un peu moins du tiers des répondants estiment que leurs compatriotes se sentent en sécurité par rapport à un attentat terroriste, alors que 57 % croient que les Américains sont inquiets et que 10 % jugent que les Américains se sentent en danger. Quand les répondants doivent se prononcer sur leur propre sentiment de sécurité, un peu plus de la moitié d'entre eux se sentent en sécurité, 40 % sont inquiets et 6 % seulement se disent en danger. À la lumière de ces résultats, il semble que les Américains surestiment l'insécurité de leurs compatriotes.

Les conclusions que tire la Commission de l'examen de ces sondages sont qu'une montée de la peur du crime serait en contradiction avec les statistiques sur la criminalité, du moins au Canada. En effet, la criminalité est en baisse depuis le début des années 1990. Selon Statistique Canada, en 2006 le taux global de criminalité a diminué de 3 %[31] (atteignant ainsi le plus bas taux de criminalité

25. LÉGER MARKETING, *Les Canadiens et la sécurité au Canada*, 2002.

26. Campbell CLARK, « Canadians Want Strict Security : Poll », *GlobeandMail.com* [en ligne], 11 août 2005. [http://www.theglobeandmail.com/servlet/story/RTGAM.20050811.wxsecurity11/BNStory/National/].

27. STRATEGIC COUNSEL, *Public Perceptions of Immigration and Terrorism*, 9 juin 2006.

28. LÉGER MARKETING, *Are Other Terrorist Attacks Imminent? September 11 from the Point of View of Canadians : 5 Years Later* – Part 1, août 2006.

29. STRATEGIC COUNSEL, *Immigration, Terrorism and National Security*, 7 août 2005.

30. Sondage New York Times-CBS News, 17-21 août 2006.

31. STATISTIQUE CANADA, « Statistiques de la criminalité au Canada, 2006 », *Juristat*, vol. 27, n° 5, 18 juillet 2007, p. 2.

en 25 ans), suivant une baisse de 5 % en 2005[32]. Cette statistique cache évidemment plusieurs réalités. Tout d'abord, le nombre de crimes violents, même si ceux-ci ne représentent que 12 % de tous les crimes commis au Canada, continue de fléchir de façon générale, et ce, depuis le milieu des années 1990[33]. De plus, le fléchissement du taux global de criminalité est largement attribuable à une baisse marquée du nombre de crimes sans violence, c'est-à-dire les crimes contre les biens et les autres infractions au Code criminel[34]. Les rapports statistiques sur la criminalité, particulièrement en ce qui concerne la criminalité liée aux nouvelles technologies de l'information, doivent être prudemment interprétés. Cette forme récente de criminalité (qui comprend notamment certaines formes de vols d'identité, par exemple) n'est pas systématiquement déclarée par les corps policiers, ce qui empêche de tracer facilement un portrait de la réalité.

Une société qui est alimentée, volontairement ou non, par une certaine insécurité est plus portée à exprimer un besoin constant d'informations pour évaluer et gérer les risques et les dangers qui la guettent. Elle met alors l'accent sur la distribution sociale des dangers et non sur celle des bénéfices : l'objectif ne consiste pas tant à répartir équitablement ce qu'il y a de bon entre les acteurs sociaux, mais plutôt à déterminer comment faire en sorte que ce qu'il y a de mauvais ne touche personne[35]. Il s'agit de la logique négative à l'œuvre dans ce qu'il est convenu d'appeler, d'après l'ouvrage phare du sociologue allemand Ulrich Beck, la société du risque.

La place du risque dans la société

L'obsession pour les risques inhérents à la vie est relativement nouvelle et les hypothèses tentant d'expliquer ses causes sont sujettes à débat. Parmi les causes qui font généralement l'objet de consensus, il faut noter la prise de conscience que le développement de la science et de la technologie offre à l'humanité d'immenses possibilités, mais également les moyens de détruire les conditions permettant la vie.

Qu'est-ce que le risque ?

La notion de risque est très répandue et son sens a pris une connotation en lien avec les préoccupations de l'ère moderne. En effet, plusieurs spécialistes de la question attirent l'attention sur l'obsession pour l'élimination des risques en tant qu'illustration de l'évolution des mentalités depuis le dernier siècle. François Ewald, par exemple, considère que c'est l'universalisation de la notion de risque qui caractérise notre siècle et la modernité. De plus, cet auteur distingue le sens du terme « risque » dans le langage courant du sens qui lui est donné dans le domaine de l'assurance notamment. Dans le premier cas, risque « est pris comme synonyme de danger, de péril, d'événement malheureux qui peut arriver à quelqu'un ; il désigne une menace objective[36] », alors que, dans le deuxième cas, le risque désigne « un mode de traitement spécifique de certains événements qui peuvent advenir à un groupe d'individus, ou plus exactement à des valeurs ou des capitaux possédés ou représentés par une collectivité d'individus, c'est-à-dire par une population[37] ». En d'autres mots, la notion de risque consiste en « une façon de se représenter les événements, de les objectiver [...][38] ».

À la lumière de cette interprétation, il est facile de comprendre pourquoi le risque constitue une notion qui touche à toutes les sphères de l'activité humaine. Qui plus est, le risque, s'il tend à l'universalisation, vise aussi la pérennité. En effet, le risque peut être vu comme un « horizon indépassable de la condition humaine[39] ». Malgré les campagnes de sensibilisation et de prévention, malgré la promulgation de lois, le travail des experts, des praticiens, pour ne nommer que quelques types d'interventions, des événements malheureux continuent de se produire.

32. STATISTIQUE CANADA, « Statistiques de la criminalité au Canada, 2005 », *Juristat*, vol. 26, n° 4, 20 juillet 2006, p. 4.
33. *Ibid.*, p. 5.
34. *Ibid.*, p. 8.
35. Richard V. ERICSON et Kevin D. HAGGERTY, *Policing the Risk Society*, Toronto, University of Toronto Press, 1997, p. 6.
36. François EWALD, *L'Etat providence*, Paris, Bernard Grasset, 1986, p. 173.
37. *Ibid.*
38. Patrick PERETTI-WATEL, *op. cit.*, p. 48.
39. David LE BRETON, *op. cit.*, p. 25-26.

En général, les sociétés occidentales se trouvent dans une position d'ambivalence au regard du risque. De manière collective, les personnes s'entendent habituellement pour réduire les risques pouvant toucher des groupes entiers. C'est pourquoi l'État agit en ce sens en élaborant des plans d'action, des politiques et des lois visant la protection des citoyens et de leur santé, mais aussi de l'environnement, par exemple. Néanmoins, sur le plan personnel, il n'est nul besoin d'être fin observateur pour constater l'attrait que suscite le risque chez certaines personnes. À la différence que, dans la plupart des cas, les risques ne sont courus que par la personne qui les prend (ce qui n'empêche pas que, ce faisant, cette personne s'expose à des conséquences fâcheuses qui peuvent à leur tour être dommageables pour son entourage, comme dans le cas d'un joueur compulsif qui perd tout). Ces risques sont nombreux et divers : sports extrêmes, pratiques sexuelles à risque, recherche de sensations fortes, jeux de hasard, consommation de drogues, etc. Il est possible d'établir un parallèle avec les nouvelles technologies de surveillance et de contrôle. D'une part, collectivement, les sociétés occidentales ont mis en place des mécanismes de protection de la vie privée et de la confidentialité des renseignements personnels. Il s'agit d'une manière parmi d'autres de réduire les risques liés à la circulation de ce type de données dans les espaces publics et privés. D'autre part, toutefois, sur le plan personnel, les utilisateurs de cartes de crédit et de débit, les adhérents à des programmes de récompenses et les personnes qui utilisent Internet pour, entre autres choses, effectuer des transactions financières prennent des risques (à titre personnel) en divulguant des renseignements personnels et pas toujours de manière sécuritaire.

Le lien entre sécurité et risque est illustré par l'anthropologue David Le Breton lorsqu'il attire l'attention sur le glissement de sens qu'a subi le terme « risque » : « Le glissement du sens du terme 'risque', passant de la référence à une probabilité à celle d'une menace ou d'un danger, est le symptôme d'une société hantée par la sécurité et soucieuse d'assurer la prévention des différentes formes d'entraves et de malheurs touchant la condition humaine[40]. » La volonté d'éliminer les risques étant une obsession des sociétés occidentales contemporaines, il est devenu courant de faire référence à ces dernières comme étant des sociétés du risque.

Les caractéristiques de la « société du risque »

Afin de respecter l'esprit de ce chapitre, qui consiste à brosser un tableau du contexte dans lequel s'inscrit le déploiement des NTSC, la société du risque sera abordée uniquement en se référant à ses principales caractéristiques[41] et en les liant à l'objet du présent avis.

Ce lien sera d'autant plus nécessaire du fait que le sociologue allemand Ulrich Beck a forgé ce concept et a élaboré une imposante réflexion à son sujet dans un autre contexte : la prise de conscience des effets néfastes de la modernisation industrielle, notamment sur l'environnement et sur la santé humaine. L'attention ne sera cependant pas mise sur ce contexte dans le présent avis, mais plutôt sur l'esprit de la société du risque et sur les moyens mis en place dans une telle société pour gérer la répartition des dangers. Les NTSC comptent parmi ces moyens.

La société du risque représente une rupture dans l'histoire des mentalités. La société préindustrielle se caractérise notamment par une conception autoritaire et dogmatique de la science, par une confiance presque sans borne en elle (dans un optimisme qui trouve son illustration la plus éclatante dans l'idée de progrès), par un fort accent mis sur la production et le partage des richesses ainsi que par des rôles sociaux et familiaux relativement figés. La société du risque entre en rupture avec cette société, « non pas par l'effet d'une critique externe, en s'appuyant sur un modèle social et politique nouveau, mais au contraire par l'approfondissement de ses propres principes[42] ». D'une part, la société du risque est consciente de la faillibilité de la science, mais plus encore : ce n'est plus seulement la nature qui engendre des risques et qu'il suffit de maîtriser, mais aussi la recherche scientifique. Par ailleurs, la production et le partage des richesses tendent de plus en plus à muter en production et en partage des risques découlant des efforts mis en œuvre dans un premier temps. Enfin, les anciens rôles sociaux sont remis en question, comme l'illustre l'exemple du mouvement de libération des femmes[43].

40. David LE BRETON, *op. cit.*, p. 23.

41. La plupart des caractéristiques présentées sont tirées de Richard V. ERICSON et Kevin D. HAGGERTY, *op. cit.*, p. 85-91.

42. Luc FERRY, « La nouvelle société du risque », dans *Liberté, risque & responsabilité : nouveaux repères à l'heure de la mondialisation et du terrorisme international*, Paris, Institut français des relations internationales, 2001, p. 20.

43. *Ibid.*, p. 22.

Dans la société du risque, l'incertitude liée aux menaces et aux dangers doit être réduite à un point où les personnes se sentent suffisamment en confiance pour agir. La notion de société du risque ne doit pas porter à confusion : il ne s'agit pas d'une société où les risques sont nécessairement plus grands, omniprésents ou avérés, mais bien d'une société plus sensible aux risques de toutes sortes[44]. En fait, la question qui caractérise la société du risque est la suivante : « Comment les risques et les menaces qui sont systématiquement produits au cours du processus de modernisation avancée peuvent-ils être supprimés, diminués, dramatisés, canalisés, et, dans le cas où ils ont pris la forme d'"effets induits latents", endigués et évacués de sorte qu'ils ne gênent pas le processus de modernisation ni ne franchissent les limites de ce qui est 'tolérable' (d'un point de vue écologique, médical, psychologique, social)[45] ? »

La logique du risque est orientée vers le futur. Évaluer les risques suppose une projection dans l'avenir. Il devient alors possible d'envisager des événements qui risquent de se produire et d'en évaluer maintenant les tenants et aboutissants :

> *La conscience que l'on a du risque ne se situe pas dans le présent, mais essentiellement dans l'avenir. Dans la société du risque, le passé perd sa fonction déterminante pour le présent. C'est l'avenir qui vient s'y substituer, et c'est alors quelque chose d'inexistant, de construit, de fictif, qui devient la « cause » de l'expérience et de l'action présentes. Aujourd'hui, nous devenons actifs pour éviter, atténuer, prévenir les problèmes ou les crises de demain ou d'après-demain – ou justement pour ne rien faire de tout cela*[46].

La société du risque est étroitement liée au développement de la science et de la technologie. Les liens entre les risques et le développement de la science et de la technologie sont multiples et complexes. Deux phénomènes parallèles sont à l'œuvre : d'une part, plus les connaissances scientifiques et technologiques avancent, plus elles jettent un éclairage sur des événements considérés jusqu'alors comme des fatalités, comme l'œuvre du destin. Dès lors, ces événements sont étiquetés comme étant des risques pouvant et devant être éradiqués ; d'autre part, le développement de la science et de la technologie crée de nouveaux risques. Beck donne une autre illustration des relations entre la société du risque et le développement de la science et de la technologie lorsqu'il affirme que, dans « leur façon d'appréhender les risques liés à l'évolution industrielle, les scientifiques dépendent des attentes et des horizons de valeurs de sociétés, de même qu'inversement la réaction sociale et la perception des risques dépendent d'arguments scientifiques[47] ». Ce qui amène à traiter d'une autre caractéristique de la société du risque.

Dans la société du risque, le discours sur le risque n'est pas l'apanage exclusif des scientifiques. Les scientifiques appelés à mesurer le risque ne sont pas les seuls à revendiquer une autorité à cet égard. Différents acteurs sociaux, selon la perception qu'ils ont d'un risque précis, prennent part au discours sur le risque pour faire contrepoids à l'évaluation scientifique des risques. Or, l'évaluation scientifique (donc, un calcul probabiliste) de ce risque peut largement différer de la perception du même risque par un groupe de citoyens, par exemple.

Plusieurs facteurs psychosociaux influencent la perception du risque. En voici quelques-uns à titre d'exemples[48] :

- **Familiarité** : les activités comportant des risques qui sont moins familiers.
- **Incertitude scientifique** : les risques qui sont moins connus de la communauté scientifique.
- **Exposition involontaire** : les risques auxquels on s'expose involontairement.
- **Potentiel de catastrophe** : les situations comportant un potentiel d'accident majeur ou de désastre.
- **Réversibilité** : les activités qui génèrent des effets irréversibles.
- **Effets sur les générations futures** : les activités qui comportent des risques pour les générations futures.
- **Équité** : les activités qui comportent des risques distribués de façon inéquitable dans la population.

44. Ulrich BECK, *La société du risque : sur la voie d'une autre modernité*, Paris, Flammarion, 2001 (1986), p. 100.
45. *Ibid.*, p. 36.
46. *Ibid.*, p. 61.
47. *Ibid.*, p. 54-55.
48. Traduction et adaptation de Vincent T. COVELLO (1983) citée dans BUREAU D'AUDIENCES PUBLIQUES SUR L'ENVIRONNEMENT, *Le projet de la Régie intermunicipale de gestion des déchets sur l'île de Montréal*, rapport d'enquête et d'audience publique, 1993, p. 140.

- **Couverture médiatique** : les risques qui attirent l'attention des médias.
- **Contrôle** : les risques sur lesquels les gens croient ne pas avoir de contrôle.

La logique de la société du risque renferme une « éthique implicite ». Personne ne peut faire un discours sur les risques sans s'inscrire dans une éthique implicite de la société du risque et sans que son discours soit totalement dénué d'une coloration éthique, sociale, culturelle, économique et politique. L'encadré qui suit rapporte succinctement ce que Beck entend par une éthique implicite de la société du risque.

L'éthique implicite de la société du risque

Les risques dont on fait l'expérience présupposent un horizon normatif de sécurité perdue, de confiance brisée. C'est pourquoi les risques, même lorsqu'ils apparaissent muets, recouverts d'un habillage de chiffres ou de formules, restent par définition liés à un point de vue ; c'est pour cela qu'ils demeurent des poétisations mathématiques de visions déçues de la vie qui mériterait d'être vécue. Or ces poétisations elles-mêmes demandent à être crues, ce qui équivaut à dire qu'on ne peut en faire l'expérience comme ça. En ce sens, on peut dire que les risques sont en négatif les images concrétisées des utopies dans lesquelles est conservé et revitalisé ce qu'il y a d'humain dans le processus de modernisation, ou du moins ce qu'il en reste. Malgré toutes ses transformations, cet horizon normatif qui seul permet de rendre perceptible ce qu'il y a de risqué dans le risque, on ne peut l'évacuer par le recours aux mathématiques ou à l'expérimentation. Tôt ou tard, quelle que soit l'intensité de cette concrétisation, s'impose la question de l'acceptation, et avec elle l'éternelle question, toujours d'actualité : comment voulons-nous vivre ? Qu'y a-t-il de proprement humain chez l'homme, de proprement naturel dans la nature, qu'il s'agirait de préserver ? Parler de « catastrophe », c'est en ce sens exprimer de façon exacerbée, radicalisée, appliquée au concret, que cette évolution n'est pas voulue[49].

La société du risque est directement concernée par la sécurité[50]. Une grande partie des efforts des gouvernements visent à assurer la sécurité aux citoyens : sécurité alimentaire, sécurité civile, sécurité nationale, sécurité publique, sécurité routière, sécurité sanitaire, etc. Cet élan vers la sécurité stimule une demande insatiable pour une meilleure connaissance des risques. Or, plus la recherche d'informations sur les risques progresse, plus elle examine en détail les menaces et leur probabilité d'occurrence et plus elle met au jour de nouvelles zones d'insécurité[51]. Beck ajoute : « Plus les risques augmentent, plus on doit promettre de sécurité, et il faut constamment répondre aux assauts d'une opinion publique vigilante et critique par des interventions cosmétiques ou réelles sur le développement technico-économique[52]. »

En matière de sécurité nationale et publique, l'obtention d'un maximum d'informations permet de dresser des profils (celui de l'agresseur sexuel type, par exemple), de déterminer des endroits où des crimes ou des attentats terroristes ont plus de probabilités de survenir, d'identifier des catégories de personnes à surveiller plus étroitement et de perfectionner le travail des autorités policières sur le terrain, pour ne nommer que quelques exemples. Ainsi, les calculs probabilistes des experts en évaluation du risque peuvent servir à répartir efficacement les ressources là où les besoins se trouvent[53]. La collecte d'informations est, par conséquent, absolument vitale pour la société du risque. Ces informations sont obtenues, entre autres, par la surveillance.

Vers une société de surveillance ?

Afin d'assurer son bon fonctionnement, la société du risque a besoin d'informations et de moyens pour les recueillir. Parmi ces moyens figurent les nouvelles technologies de surveillance et de contrôle. Elles constituent des outils précieux afin de dresser la cartographie des risques et d'évaluer la nature et la quantité de ressources devant être allouées aux différents secteurs de l'activité humaine.

49. Ulrich BECK, *op. cit.*, p. 51.

50. Pour une analyse plus approfondie de la notion de sécurité, voir le document de réflexion de la COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE, *L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques*, Sainte-Foy, 2005, p. 1-3.

51. Richard V. ERICSON et Kevin D. HAGGERTY, *op. cit.*, p. 85.

52. Ulrich BECK, *op. cit.*, p. 37.

53. SURVEILLANCE STUDIES NETWORK, *A Report on the Surveillance Society*, Grande-Bretagne, septembre 2006, p. 7. [http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf].

Récemment, et surtout en réaction aux événements du 11 septembre 2001, un changement de cap est observable dans les méthodes de collecte de renseignements. L'objet de la surveillance ne se limite plus à quelques segments de la population déjà considérés comme « à risque ». C'est maintenant la population en général qui est placée sous surveillance afin de cibler des interventions vers les personnes jugées à risque ou qui posent des risques pour d'autres personnes[54]. Ce qui fait dire à certains qu'il n'est pas pertinent d'entrevoir la société de surveillance pour le futur ou encore comme une utopie : les sociétés actuelles sont déjà des sociétés de surveillance[55].

Toutefois, la surveillance ne constitue pas un phénomène nouveau et elle n'a pas attendu l'avènement d'une société du risque ou de technologies raffinées pour se manifester. La surveillance est reconnue comme partie intégrante de toutes les sociétés humaines depuis des temps immémoriaux, puisque le simple acte de socialisation serait impensable sans la surveillance exercée par les adultes. L'enfant apprend à interagir avec les autres sous la supervision d'adultes qui exercent à son endroit une surveillance. À un autre degré, la surveillance peut aussi être considérée comme un mécanisme central à travers lequel l'État moderne accomplit ses fonctions administratives entourant la santé, le bien-être, l'éducation et la sécurité de sa population[56].

Qu'est-ce que la surveillance ?

Les définitions de la surveillance sont nombreuses ; certaines sont englobantes, d'autres rendent bien toute la complexité du phénomène. Une définition générale, qui s'applique tout autant au domaine de la sécurité, pourrait se formuler ainsi : la surveillance est la collecte et le traitement de renseignements (qu'ils permettent ou non d'identifier des personnes) dans le but d'influencer ou de superviser[57].

Une autre définition retenue se veut plus substantielle. Selon cette définition, l'exercice de la surveillance comporte une ou plusieurs des activités suivantes :

- la collecte et le stockage de l'information concernant des personnes ou des objets ;
- la supervision des activités des personnes ou des objets à travers la transmission d'instructions ou l'architecture d'endroits ;
- l'application des activités de collecte d'informations à la tâche de régulation du comportement des personnes faisant l'objet d'une surveillance et, dans le cas de personnes, de leur obéissance aux instructions[58].

Enfin, il faut mentionner une dernière définition qui semble aller encore plus loin dans la description de certaines caractéristiques de la surveillance. Ainsi, lorsqu'une attention intéressée, routinière et systématique est portée à des renseignements personnels, pour des raisons de contrôle, de gestion, d'influence ou de protection, il est pertinent de parler de surveillance. Cette définition est précisée par les éléments qui suivent.

- L'attention est intéressée : la surveillance est justifiée dans une optique de contrôle, de gestion ou dans un autre but collectivement admis ;
- Elle est routinière : la surveillance est imbriquée dans la vie quotidienne ;
- Elle est également systématique : la surveillance est planifiée et se déroule selon un horaire préétabli et rationnel ;
- Enfin, elle s'intéresse à l'information et aux renseignements précis : bien que certaines formes de surveillance soient tributaires de données agrégées, la plupart ont trait à des personnes identifiables dont les données sont collectées, stockées, transmises, récupérées, comparées, forées et échangées[59].

L'effet contrôlant de la surveillance peut parfois être indirect et non intentionnel[60]. En outre, plusieurs formes de surveillance s'avèrent légitimes dans un cadre démocratique, quoique leur impact cumulatif sur le respect de la vie privée des personnes demeure une source de préoccupation[61].

54. *Ibid.*, p. 12.
55. *Ibid.*, p. 1.
56. Clive NORRIS et Gary ARMSTRONG, *The Maximum Surveillance Society : The Rise of CCTV*, Oxford, Berg, 1999, p. 4.
57. David LYON, *Surveillance Society : Monitoring Everyday Life*, Buckingham, Open University Press, 2001, p. 2.
58. Christopher DANDEKER, *Surveillance, Power and Modernity*, New York, St. Martin's Press, 1990, p. 37.
59. SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 4.
60. *Ibid.*, p. 33.
61. David H. FLAHERTY, *Protecting Privacy in Surveillance Societies*, Chapel Hill, University of North Carolina Press, 1989, p. 1.

Les caractéristiques de la société de surveillance

La montée d'une société de surveillance se situe dans la continuité de la modernité[62]. Cette dernière se caractérise notamment par l'importance accordée à la valeur d'efficacité. Concrètement, cela se traduit par des pratiques organisationnelles visant à répondre convenablement et rapidement aux besoins d'une population qui exige de l'État qu'il prenne en charge certains de ses besoins (santé, sécurité, bien-être, éducation, etc.) et qui est à l'affût de produits de consommation répondant toujours mieux à ses demandes. À cette fin, les organisations mettent en place un appareil bureaucratique à la recherche d'informations lui permettant de mieux connaître leur « clientèle », de satisfaire, voire d'anticiper ses besoins. Cette bureaucratie, qui vise toujours plus de rapidité dans l'exécution et de contrôle sur le processus de traitement de l'information, met en place des mécanismes de surveillance afin de l'alimenter en information utile. Bref, la surveillance a beaucoup à voir avec la manière dont les sociétés modernes se structurent, en l'occurrence sur les plans politique et économique, en valorisant la mobilité, la vitesse, la sécurité et la liberté des consommateurs.

Bien que le déploiement des NTSC soit souvent associé par les médias au développement d'une société plus autoritaire (sinon totalitaire), sa justification s'articule davantage dans une logique de protection du citoyen[63]. Cela dit, il y a tout de même lieu de s'inquiéter d'un tel déploiement, de la manière dont il se déroule et des conséquences qu'il peut avoir.

Une autre caractéristique de la société de surveillance est qu'elle est étroitement liée à la technologie. Cela ne signifie cependant pas que l'une soit la cause de l'autre. Bien entendu, les êtres humains n'ont pas attendu l'arrivée de telles technologies pour se surveiller les uns les autres. Le fait est qu'autrefois la surveillance était non généralisée et non systématique, alors que de nos jours elle est routinière, courante. La surveillance s'inscrit dans la vie quotidienne et elle est habituellement mise en place par des agences et des organisations éloignées de nous géographiquement parlant, grâce aux possibilités qu'entraîne le développement technologique.

En outre, la surveillance fait l'objet d'un phénomène de généralisation, et ce, sur plusieurs plans. D'abord, la surveillance ne s'intéresse plus seulement aux déviants et aux suspects. Toute personne peut faire l'objet de surveillance. Amasser une grande quantité d'informations permet de dresser des profils plus complets, dans tous les domaines imaginables. L'exemple de la lutte au terrorisme est éclairant à cet égard. Tant que la surveillance se limite à garder un œil sur des suspects et sur des personnes qui semblent associées à des groupes terroristes, les personnes qui ne correspondent pas à ce « profil » passent inaperçues. Mais en surveillant, par exemple, les habitudes de navigation sur Internet de tous les citoyens, les autorités seraient en mesure de repérer des internautes louches par les visites qu'ils font de sites liés à des groupes terroristes ou encore de sites donnant le mode d'emploi pour confectionner une bombe, par exemple. Mais, surtout, en comparant les habitudes de navigation sur Internet de criminels et de terroristes, les autorités seraient en mesure de dresser un profil de navigation du « terroriste type ». Le même exercice pourrait être fait avec les fraudeurs, les pédophiles, etc. Mais le principe demeure le même : pour arrêter des criminels avant même qu'ils ne commettent une infraction, pour effectuer une prévention encore plus englobante et efficace, il faut pouvoir surveiller le plus grand nombre de personnes et, idéalement, la population en entier.

Un tel projet exige évidemment que la surveillance soit presque omniprésente et quasi constante. Il s'agit d'un autre mode de généralisation de la surveillance qui tend donc à s'effectuer à peu près partout et presque continuellement. Ce qui fait dire à certains que, désormais, la vie quotidienne est sujette à la surveillance. Il serait difficile de penser à un endroit ou à une activité qui soit à l'abri de toute surveillance[64]. De plus, les acteurs qui opèrent des mécanismes de surveillance tendent à se multiplier. Non seulement l'État, mais les entreprises privées et les citoyens, à titre personnel, utilisent les NTSC à des fins diverses, dont la sécurité.

Tout un pan de la littérature et du cinéma a introduit dans la population des craintes qui, si elles ne peuvent être facilement écartées du revers de la main, méritent tout au moins d'être mises en perspective. Le portrait

62. *Ibid.*, p. 1 et 2.

63. Clive NORRIS et Gary ARMSTRONG, *op. cit.*, p. 4.

64. David LYON, *Surveillance Society : Monitoring Everyday Life*, Buckingham, Open University Press, 2001, p. 1.

qui est habituellement fait de la surveillance pourrait laisser croire à une vaste conspiration visant le contrôle total des populations. Deux pièges guettent les adhérents à cette théorie du complot : croire que la surveillance est une machination des puissants de ce monde et penser que la surveillance est une conséquence directe du développement de la science et de la technologie[65].

Ce n'est pas vraiment l'apparition imminente d'un *Big Brother* qui inquiète la Commission. En fait, c'est l'avènement de nombreux *Small Brothers*, c'est-à-dire de plusieurs organismes et personnes qui, à titre privé, se mettent à faire de la surveillance à des fins de sécurité, qui est préoccupant. Ce genre de surveillance qui ne respecte pas nécessairement toujours les lignes directrices et les bonnes pratiques en la matière risque d'échapper totalement au contrôle de l'État.

Le cadre éthique : les enjeux et les valeurs en cause

Le cadre éthique dans lequel la Commission campe son analyse s'appuie sur deux considérations : tout d'abord, puisque la Commission a toujours privilégié une approche par les valeurs, il lui apparaissait primordial de commencer en donnant une brève signification de celles qui sont évoquées dans le présent avis ; de plus, la Commission tenait dès à présent à définir brièvement les principaux enjeux éthiques soulevés par le déploiement des NTSC. Ces enjeux sont analysés plus en profondeur au chapitre trois.

Les valeurs

Dans les sociétés démocratiques libérales, la valeur d'autonomie joue un rôle central. L'autonomie est cette valeur qui permet aux personnes de mener et d'accomplir un projet de vie comme bon leur semble, dans les limites imposées par les droits et libertés des autres personnes. Dans le présent avis, elle se traduit comme étant l'expression de la liberté des citoyens vivant dans des sociétés démocratiques, notamment par rapport au regard, qui peut parfois être intrusif, de l'État et d'autres organisations. Bref, « personne ne possède l'autonomie, si elle est soumise à la volonté d'autrui[66] ». Concrètement, plus les citoyens participeront à l'élaboration, à la mise en place et au suivi des balises entourant le déploiement des NTSC, plus ce processus sera conforme à l'idéal démocratique.

Cette volonté de privilégier l'autonomie des personnes dans les démocraties libérales se manifeste plus concrètement par l'attachement à toute une constellation de valeurs fondamentales. Bien que ces valeurs puissent, dans certains cas précis, entrer en conflit, il convient de reconnaître qu'elles ont un point en commun. Elles rendent possibles l'autonomie et, partant, la vie démocratique. Parmi cet ensemble de valeurs, la Commission a retenu celles qu'elle estimait les plus concernées par le déploiement des NTSC, c'est-à-dire la sécurité, la liberté, la vie privée, la transparence, la justice et l'égalité.

Les valeurs de sécurité et de liberté constituent probablement celles qui viennent le plus spontanément en tête considérant l'objet du présent avis. Elles sont étroitement liées à la vie démocratique. D'une manière générale, il est possible de concevoir les démocraties modernes comme autant d'équilibres plus ou moins réussis entre le pouvoir de l'État en matière de sécurité et les droits et libertés des citoyens. Afin d'exercer leur souveraineté, conformément à la doctrine politique qu'est la démocratie, les citoyens renoncent délibérément à certaines pratiques (comme celle de se faire justice eux-mêmes, par exemple). En contrepartie, ils prennent le pari de garantir le respect d'autres droits et libertés jugés fondamentaux (liberté d'expression, de mouvement, droit à la vie privée, droit à l'intégrité physique, etc.). Le rôle de l'État devient alors comparable à celui d'un « arbitre protecteur du citoyen ». Son pouvoir de coercition permet à tout un chacun de profiter de certaines libertés et de revendiquer certains droits sans craindre que son voisin ne l'en prive. Par exemple, si un citoyen désire voter pour un candidat plutôt qu'un autre, c'est l'État qui met en œuvre les moyens afin que cette volonté puisse s'exprimer sans craindre diverses formes d'intimidation d'opposants.

La vie privée est aussi une valeur étroitement associée aux divers discours entourant le déploiement des NTSC. Le respect de la vie privée est considéré aujourd'hui comme un droit fondamental. Il n'en a pas toujours été ainsi. À travers l'histoire, la limite entre la sphère privée

65. SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 2.

66. Laurence THOMAS, « Autonomie de la personne », dans Monique CANTO-SPERBER (dir.), *Dictionnaire d'éthique et de philosophie morale*, Paris, Presses Universitaires de France, 2001 (1996), p. 121.

et la sphère publique a fluctué. Pour certains, la période actuelle, soit l'époque moderne, se caractérise par une montée de l'individualisme qui fait en sorte que les personnes se renferment dans une sphère privée de plus en plus grande, au détriment d'une participation active à la vie publique[67]. Il faut aussi rester bien conscient que cette analyse perd de vue l'importante lutte qui se joue entre l'État et les citoyens. La pression toujours plus forte de l'État pour une surveillance plus serrée des citoyens encourage ces derniers à se prémunir des incursions dans leur vie privée avec un zèle tout aussi grandissant.

Historiquement, le développement du respect de la vie privée est associé au droit d'être laissé seul et au droit à l'intimité[68]. La valorisation croissante du respect de la vie privée est aussi liée au développement de l'individualisme, et ce, tant à travers la pensée philosophique moderne que par des phénomènes socio-historiques comme la modification de l'habitation au Moyen Âge (qui permet aux individus de s'isoler dans des pièces séparées) et la montée d'une nouvelle classe socio-économique, la bourgeoisie (celle-ci ayant les moyens financiers d'aménager ses habitations de manière à respecter l'intimité des membres de la famille). Dans les sociétés de l'information, le respect de la vie privée passe désormais moins par la protection individuelle de l'intimité et des informations personnelles et davantage par « le droit de contrôler l'usage que les autres font des informations qui me regardent[69] ».

Le respect de la vie privée est un concept qui demeure difficile à définir tellement il prête à interprétation. Plutôt que de chercher à définir précisément ce concept, la Commission a réuni quelques aspects généraux le caractérisant et qui font généralement consensus. Ainsi, le respect de la vie privée peut renvoyer au droit à être laissé seul, à l'accès limité au soi, au secret, au contrôle de l'information personnelle, à la personnalité et à l'intimité[70]. De plus, la vie privée peut être divisée en quatre aspects généraux :

- La vie privée informationnelle. Elle est associée à l'élaboration de normes régissant la collecte et la gestion des renseignements personnels ;
- La vie privée corporelle. Elle correspond à la protection physique de la personne contre des procédures intrusives comme les fouilles et les tests génétiques, par exemple ;
- La vie privée communicationnelle. Elle couvre la sécurité des communications par téléphone ou par courriel par exemple ;
- La vie privée territoriale. Elle se définit par la mise en place de frontières contre l'intrusion dans des contextes tels que la maison ou le lieu de travail[71].

La transparence « est une valeur démocratique essentielle à la gouvernance publique ; elle témoigne d'une approche non paternaliste qui invite à une responsabilisation des divers acteurs sociaux[72] ». Aussi, s'inspirant de ce qu'elle avait dit dans un précédent avis, la Commission réaffirme l'importance de cette valeur qui traduit la volonté de voir un déploiement des NTSC se faire non pas dans une zone d'ombre, mais plutôt en partenariat avec des acteurs du milieu et des citoyens bien informés des principaux enjeux.

Elle fait également appel aux valeurs de justice et d'égalité, notamment au regard du traitement des renseignements personnels. Le recours à des techniques comme le profilage ou le ciblage de certaines catégories de personnes en vue d'améliorer l'efficacité de la surveillance peut accroître les risques de discrimination et de stigmatisation. Or, il demeure essentiel que les citoyens sous surveillance soient traités en accord avec les valeurs de justice et d'égalité afin d'éviter de subir des préjudices qui peuvent être difficiles à réparer.

67. Pour une liste des auteurs appartenant à cette école de pensée, voir Elia ZUREIK, Lynda HARLING STALKER et Emily SMITH, *Background Paper for the Globalization of Personal Data Project : International Survey on Privacy and Surveillance*, Kingston, Queen's University, 2006, p. 3 et 4.

68. Stefano RODOTA, « Privée (Protection de la vie) », dans Gilbert HOTTOIS et Jean-Noël MISSA (dir.), *Nouvelle encyclopédie de bioéthique*, Bruxelles, De Boeck Université, 2001, p. 665.

69. *Ibid.*, p. 666.

70. Elia ZUREIK, Lynda HARLING STALKER et Emily SMITH, *op. cit.*, p. 1 et 2.

71. PRIVACY INTERNATIONAL, *Overview of Privacy*, [en ligne], 29 octobre 2006. [http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-543673&als[theme]=Privacy%20and%20Human%20Rights].

72. COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE, *Pour une gestion éthique des OGM*, Sainte-Foy, 2003, p. 63.

Les enjeux éthiques

La Commission n'a pas la prétention de couvrir le vaste ensemble des enjeux éthiques soulevés par cette pratique. Néanmoins, les suivants lui sont apparus comme les principaux par rapport à son mandat.

- L'évaluation de la pertinence, de l'efficacité et de la fiabilité des NTSC

Pour assurer la légitimité de leur déploiement, les NTSC doivent être jugées pertinentes, efficaces et fiables. Le critère de *pertinence* consiste à savoir si les NTSC s'avèrent le meilleur moyen pour répondre au besoin reconnu en matière de sécurité. Pour que les NTSC soient *efficaces*, il faut que les résultats obtenus par leur déploiement correspondent aux visées d'origine. Dans cette perspective, il faudrait que les NTSC atteignent un niveau de performance supérieur pour éviter de causer des préjudices à des personnes innocentes. Ces questions, bien qu'elles soient d'ordre technique, exigent des reponses. Les mécanismes d'évaluation et leurs résultats doivent être facilement accessibles à la population dans une forme facile à comprendre. À cet égard, la valeur de transparence à l'endroit de la population occupe donc une place prépondérante. De plus, les NTSC doivent être *fiables*, c'est-à-dire qu'il faut éviter que leur fonctionnement ne soulève plus de problèmes qu'elles n'apportent de solutions. Le déploiement de technologies perçues comme fiables et qui contribueraient à répandre un faux sentiment de sécurité dans la population serait inacceptable.

- La proportionnalité de la réponse à l'insécurité

Une demande insatiable de sécurité venant de la population et des spécialistes des technologies pourrait conduire à un déploiement des NTSC disproportionné avec la réalité des risques. La mise en place de NTSC doit chercher à atteindre un niveau de sécurité jugé acceptable, sans verser dans la surenchère sécuritaire. Il y a donc un équilibre à atteindre, qui exige le dialogue entre les divers acteurs du milieu et la population afin d'en arriver à des consensus sur le sujet.

- L'acceptabilité sociale

Il est difficile de déterminer le véritable niveau d'acceptabilité sociale du déploiement des NTSC. Une meilleure connaissance des perceptions et des opinions de la population en cette matière contribuerait certainement à y voir plus clair. Il est important que soient mieux connues les perspectives des citoyens à l'égard des NTSC. Il apparaît primordial de donner la parole à celles et ceux qui seront placés sous surveillance afin de favoriser un déploiement acceptable pour la société et accepté par la société.

- Le consentement

Le consentement, qui constitue toujours un enjeu important, comporte de nombreux défis. Cela est aussi vrai du consentement en matière de NTSC. Compte tenu de la nature même des NTSC, il est parfois difficile, même impossible d'obtenir un consentement individuel, libre et éclairé des personnes surveillées. En fait, le consentement libre et éclairé, sur une base individuelle, n'est tout simplement pas un concept opérationnel lorsque vient le temps de l'appliquer aux NTSC. Des données biométriques peuvent être recueillies à l'insu des personnes, des caméras de surveillance peuvent capter des images dans une rue d'un centre-ville sans que tous les passants y aient consenti, l'implantation d'une puce d'IRF sous-cutanée peut s'avérer presque impossible à refuser par certaines catégories de personnes. Différentes dispositions légales encadrent déjà le consentement à la collecte et à la communication des renseignements personnels recueillis par des NTSC. Cependant, certaines de ces dispositions comportent des limites.

- Le respect des finalités

Le respect des finalités explicitées pour lesquelles les NTSC sont déployées et l'exploitation de toutes les utilisations possibles de ces dernières sont source de tensions. D'une part, le respect des finalités explicitées est un principe important qui vise à prévenir les détournements d'usage ainsi que certaines formes d'abus et de dérives. D'autre part, l'exploitation de toutes les utilisations possibles des NTSC (y compris des fins auxquelles les personnes n'ont pas consenti) permettrait probablement d'accroître la sécurité. Mais les promesses que fait miroiter le déploiement des NTSC sont-elles en accord avec le respect des valeurs fondamentales au sein des sociétés démocratiques?

- La protection des renseignements personnels

Enjeu majeur s'il en est un, la protection des renseignements personnels renvoie inévitablement aux valeurs de vie privée et de sécurité. Cet enjeu se pose avec suffisamment de nuances selon qu'il est question de données

biométriques, de vidéosurveillance et d'identification par radiofréquence pour que la Commission en traite de manière séparée. La Commission rappelle les promesses et les risques associés au déploiement des NTSC, ce qui met en lumière à la fois le potentiel pour la gestion des risques et l'intrusion de ces technologies dans la vie privée.

Les espaces publics et privés : une frontière ténue

La frontière entre les espaces publics et les espaces privés est de plus en plus perméable. Cette observation a des répercussions sur le plan éthique, car elle signifie que l'importance accordée à la valeur de vie privée est de plus en plus matière à débat, sinon remise en question.

L'importance et la fonction des espaces privés et des espaces publics ont grandement évolué au cours des époques, à l'instar de la frontière qui les sépare. Autrefois, la montée de la religion chrétienne et plus tard celle de la classe sociale bourgeoise et du capitalisme ont modifié en profondeur la définition des concepts d'espaces privés et publics. Mais toujours ces notions se sont construites de façon interdépendante[73].

Aujourd'hui, la société de consommation et la révolution des technologies de l'information et des communications ont grandement contribué à refaçonner le concept de vie privée et, ce faisant, à brouiller la frontière qui distingue les espaces privés des espaces publics. À titre d'exemple, des organisations du secteur public et d'autres du secteur privé échangent des informations, partagent des intérêts et de plus en plus de mandats du gouvernement sont menés à bien par la combinaison des efforts des secteurs public et privé, de même que des organisations non gouvernementales[74].

Une autre illustration de l'étanchéité vacillante de cette frontière réside dans la facilité avec laquelle des données autrefois considérées comme strictement privées circulent désormais dans des systèmes informatiques publics (accès aux programmes gouvernementaux, par exemple) et privés (dossier de client chez des détaillants, par exemple)[75]. Ces renseignements peuvent toujours être considérés comme personnels ; il n'empêche que leur circulation en dehors de la sphère privée est désormais quasi quotidienne.

Enfin, il faut aussi mentionner que l'arrivée d'Internet a profondément bouleversé le rapport des personnes à leur vie privée. Par exemple, il est possible de mettre en ligne des albums de photos, des extraits vidéo et de raconter sa vie sur des blogues, autant de pratiques qui dévoilent plusieurs aspects de la vie privée des individus. Les gens sont-ils plus exhibitionnistes ou plus voyeurs qu'auparavant ? Sont-ce là des tendances qui se sont accentuées par l'arrivée d'Internet ? Sommes-nous à l'aube d'une redéfinition de la vie privée ? Chose certaine, ces questions ont accompagné la Commission tout au long de ses délibérations.

Les instruments normatifs en place

Comme le concept de renseignement personnel revient régulièrement dans le discours de la Commission en matière de NTSC et que l'utilisation de certaines technologies (notamment l'identification par radiofréquence) pose des enjeux juridiques en lien avec sa définition, il est apparu essentiel de rappeler les définitions pertinentes sur le plan juridique. De plus, les principales lois qui encadrent le déploiement des NTSC et la collecte, l'utilisation, la communication et la conservation des renseignements personnels sont signalées.

La définition juridique du renseignement personnel

Au Québec, la Loi sur la protection des renseignements personnels dans le secteur privé définit un renseignement personnel comme étant « tout renseignement qui concerne une personne physique et permet de l'identifier[76] ». Avec sensiblement les mêmes mots, la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels donne la définition suivante de l'expression « renseignement personnel » : « Dans un document, sont personnels les renseignements qui concernent une personne physique et permettent de l'identifier[77]. » Il est important de préciser que,

73. David LYON, *The Electronic Eye*, Minneapolis, University of Minnesota Press, 1994, p. 183-184.

74. SURVEILLANCE STUDIES NETWORK, *op. cit.*, p. 36.

75. David LYON, *Surveillance Society : Monitoring Everyday Life*, Buckingham, Open University Press, 2001, p. 17.

76. L.R.Q., c. P-39.1, 1993, c. 17, a. 2.

77. L.R.Q., chapitre A-2.1, 1982, c. 30, a. 54 ; 2006, c. 22, a. 110.

généralement, les renseignements personnels sont confidentiels à moins que « la personne concernée par ces renseignements [ne] consent[e] à leur divulgation[78] ».

Au Canada, la Loi sur la protection des renseignements personnels définit comme suit les renseignements personnels :

Les renseignements, quels que soient leur forme et leur support, concernant un individu identifiable, notamment :

a) les renseignements relatifs à sa race, à son origine nationale ou ethnique, à sa couleur, à sa religion, à son âge ou à sa situation de famille ;

b) les renseignements relatifs à son éducation, à son dossier médical, à son casier judiciaire, à ses antécédents professionnels ou à des opérations financières auxquelles il a participé ;

c) tout numéro ou symbole, ou toute autre indication identificatrice, qui lui est propre ;

d) son adresse, ses empreintes digitales ou son groupe sanguin ;

e) ses opinions ou ses idées personnelles, à l'exclusion de celles qui portent sur un autre individu ou sur une proposition de subvention, de récompense ou de prix à octroyer à un autre individu par une institution fédérale, ou subdivision de celle-ci visée par règlement ;

f) toute correspondance de nature, implicitement ou explicitement, privée ou confidentielle envoyée par lui à une institution fédérale, ainsi que les réponses de l'institution dans la mesure où elles révèlent le contenu de la correspondance de l'expéditeur ;

g) les idées ou opinions d'autrui sur lui ;

h) les idées ou opinions d'un autre individu qui portent sur une proposition de subvention, de récompense ou de prix à lui octroyer par une institution, ou subdivision de celle-ci, visée à l'alinéa e), à l'exclusion du nom de cet autre individu si ce nom est mentionné avec les idées ou opinions ;

i) son nom lorsque celui-ci est mentionné avec d'autres renseignements personnels le concernant ou lorsque la seule divulgation du nom révélerait des renseignements à son sujet [...][79].

La Loi sur la protection des renseignements personnels et les documents électroniques, pour sa part, définit ce qu'est un renseignement personnel de la façon suivante : « Tout renseignement concernant un individu identifiable, à l'exclusion du nom et du titre d'un employé d'une organisation et des adresse et numéro de téléphone de son lieu de travail[80]. »

En Europe, la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données donne une définition très large de ce que constitue une donnée à caractère personnel : « toute information concernant une personne physique identifiée ou identifiable (personne concernée) ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale [...][81] ».

La protection de la vie privée et des renseignements personnels à l'échelle québécoise[82]

Au Québec, l'article 5 de la Charte des droits et libertés de la personne et les articles 35 à 41 du Code civil garantissent à toute personne le droit au respect de sa vie privée.

78. L.R.Q., chapitre A-2.1, 1982, c. 30, a. 53 ; 1985, c. 30, a. 3 ; 1989, c. 54, a. 150 ; 1990, c. 57, a. 11 ; 2006, c. 22, a. 29.

79. L.R.C., 1985, ch. P-21, a. 3.

80. *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C., 2000, ch. 5, P-8.6, partie 1, a. 2.

81. PARLEMENT EUROPÉEN ET CONSEIL DE L'EUROPE, « Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données », publiée dans le *Journal officiel*, n° L 281 du 23/11/1995, p. 0031 – 0050. [http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:FR:HTML].

82. La Commission remercie Me Danielle Parent pour sa collaboration au contenu de cette section du texte.

La législation québécoise précise des obligations qui doivent s'appliquer à la collecte, à l'utilisation, à la conservation et à la communication de renseignements personnels. Ces obligations sont précisées dans les lois suivantes :

La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., chapitre A-2.1) – Cette loi s'applique aux documents détenus par un organisme public dans l'exercice de ses fonctions, que leur conservation soit assurée par l'organisme public ou par un tiers, et elle encadre l'accès à ces documents.

La Loi sur la protection des renseignements personnels dans le secteur privé (L.R.Q., chapitre P-39.1) – Cette loi établit des règles particulières à l'égard des renseignements personnels sur autrui qu'une personne recueille, détient, utilise ou communique à des tiers à l'occasion de l'exploitation d'une entreprise.

La Loi concernant le cadre juridique des technologies de l'information (L.R.Q., chapitre C-1.1) – Cette loi a pour objet d'assurer :

- « la sécurité juridique des communications effectuées par les personnes, les associations, les sociétés ou l'État au moyen de documents quels qu'en soient les supports ;
- la cohérence des règles de droit et leur application aux communications effectuées au moyen de documents qui sont sur des supports faisant appel aux technologies de l'information, qu'elles soient électronique, magnétique, optique, sans fil ou autres ou faisant appel à une combinaison de technologies ;
- l'équivalence fonctionnelle des documents et leur valeur juridique, quels que soient les supports des documents, ainsi que l'interchangeabilité des supports et des technologies qui les portent ;
- le lien entre une personne, une association, une société ou l'État et un document technologique, par tout moyen qui permet de les relier, dont la signature, ou qui permet de les identifier et, au besoin, de les localiser, dont la certification ;
- la concertation en vue de l'harmonisation des systèmes, des normes et des standards techniques permettant la communication au moyen de documents technologiques et l'interopérabilité des supports et des technologies de l'information[83]. »

La Loi sur la sécurité privée (L.R.Q., chapitre S-3.5) – Cette loi (dont quelques dispositions seulement sont en vigueur pour l'instant) s'applique à certaines activités de sécurité privée dont les suivantes sont pertinentes par rapport à l'objet du présent avis :

- « le gardiennage, soit la surveillance ou la protection de personnes, de biens ou de lieux principalement à des fins de prévention de la criminalité et de maintien de l'ordre ;
- les activités reliées aux systèmes électroniques de sécurité, soit l'installation, la réparation, l'entretien et la surveillance continue à distance de systèmes d'alarme contre le vol ou l'intrusion, de systèmes de surveillance vidéo ou de systèmes de contrôle d'accès, à l'exception d'un système sur un véhicule routier [...][84] »

Enfin, le Québec se démarque par le cadre juridique qu'il a mis en place pour protéger les citoyens en matière de biométrie. Depuis 2001, la Loi concernant le cadre juridique des technologies de l'information répond en partie aux inquiétudes que soulève le recours à la biométrie. Ainsi, conformément à l'article 44 de cette loi, un organisme public ou privé ne peut obliger une personne à établir son identité au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques. Pour avoir recours à un tel procédé, un consentement exprès de la personne doit être obtenu. De plus, la saisie de données biométriques doit se limiter à ce qui est strictement nécessaire et elle ne doit pas être faite à l'insu de la personne. L'article 45 de cette loi ajoute aux obligations des organismes celle de divulguer à la Commission d'accès à l'information (CAI) la création de toute banque de caractéristiques ou de mesures biométriques. Toujours en vertu de cette disposition, la CAI possède divers pouvoirs qui lui permettent, par exemple, de suspendre ou d'interdire la mise en service d'une base de données biométriques ou même d'en ordonner la destruction.

83. L.R.Q., chapitre C-1.1, 2001, c. 32, a. 1.

84. L.R.Q., chapitre S-3.5, 2006, c. 23, a. 1.

Dans la foulée de son document d'analyse[85], la CAI a défini neuf principes d'application de la biométrie qui découlent des effets combinés de ces trois lois québécoises. Ces principes, accompagnés d'une série de questions pour guider toute personne souhaitant utiliser la biométrie au sein de son organisation, sont[86] :

1) les solutions de rechange à la biométrie ;

2) le caractère indispensable des renseignements recueillis ;

3) la collecte auprès de la personne concernée ;

4) le consentement à l'utilisation de la biométrie ;

5) la conservation et la sécurité des données biométriques ;

6) l'utilisation des données biométriques ;

7) la communication de données biométriques ;

8) la destruction de données biométriques ;

9) les droits d'accès et de rectification.

En plus des lois existantes déjà mentionnées qui s'appliquent à la collecte, à l'utilisation, à la conservation et à la communication de renseignements personnels, tant dans le secteur public qu'au privé, le Québec, par l'entremise de la CAI, a élaboré un ensemble de règles d'utilisation de la vidéosurveillance avec enregistrement dans les lieux publics par les organismes publics[87].

Au moment de sa consultation publique sur la vidéosurveillance, la CAI avait déjà rédigé une version moins complète de ces règles et elle avait profité de l'occasion pour lancer le débat sur l'encadrement normatif de la vidéosurveillance. La voie que privilégiait la majorité des acteurs consultés était l'adoption d'une politique cadre ou d'une loi afin de « soumettre à un mécanisme juridique contraignant l'utilisation de la vidéosurveillance » et de « ne pas s'en remettre au seul jugement des administrateurs des organismes publics pour décider d'utiliser ou non la vidéosurveillance[88] ».

En matière d'identification par radiofréquence, aucune disposition légale portant spécifiquement sur cette technologie n'a pu être relevée dans les lois et règlements du Québec. Il faut toutefois signaler la publication d'un document d'analyse[89] de la CAI qui constitue en quelque sorte le début de la réflexion sur l'encadrement de l'identification par radiofréquence.

La protection de la vie privée et des renseignements personnels à l'échelle canadienne

Au niveau fédéral, l'article 8 de la Charte canadienne des droits et libertés et la partie 6 du Code criminel inscrivent le respect de la vie privée comme un droit fondamental.

La législation fédérale comporte également un ensemble de textes juridiques qui encadrent de façon générale la collecte, l'utilisation, la conservation et la communication de renseignements personnels. En effet, le Canada s'est doté de deux lois en matière de protection des renseignements personnels :

La Loi sur la protection des renseignements personnels (L.R.C., 1985, ch. P-21) – Cette loi a pour objet de compléter la législation canadienne en matière de protection des renseignements personnels relevant des institutions fédérales et de droit d'accès des individus aux renseignements personnels qui les concernent.

La Loi sur la protection des renseignements personnels et les documents électroniques (L.C., 2000, ch. 5) – Cette loi vise « à faciliter et à promouvoir le commerce électronique en protégeant les renseignements personnels recueillis, utilisés ou communiqués dans certaines circonstances, en prévoyant l'utilisation de moyens électroniques pour communiquer ou enregistrer de l'information et des transactions[90] ». Les deux premières parties de la loi ont chacune un objet différent :

85. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *La biométrie au Québec : les enjeux*, Document d'analyse, juillet 2002. [http://www.cai.gouv.qc.ca/06_documentation/01_pdf/biom_enj.pdf].

86. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *La biométrie au Québec : les principes d'application pour un choix éclairé*, juillet 2002.

87. Voir l'annexe 1.

88. Michel LAPORTE, *Bilan*, Consultation publique : l'utilisation de caméras de surveillance par les organismes publics dans les lieux publics, Commission d'accès à l'information, [en ligne], avril 2004, p. 35 et 36. [http://www.cai.gouv.qc.ca/06_documentation/01_pdf/bilan.pdf].

89. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *La technologie d'identification par radiofréquence (RFID) : doit-on s'en méfier ?*, Document d'analyse, mai 2006. [http://www.cai.gouv.qc.ca/06_documentation/01_pdf/Analyse_RFID.pdf].

90. *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C., 2000, ch. 5, P-8.6.

- La première partie a pour objet « de fixer, dans une ère où la technologie facilite de plus en plus la circulation et l'échange de renseignements, des règles régissant la collecte, l'utilisation et la communication de renseignements personnels d'une manière qui tient compte du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances. »
- La deuxième partie a pour objet « de prévoir l'utilisation de moyens électroniques, de la manière prévue dans la présente partie, dans les cas où les textes législatifs envisagent l'utilisation d'un support papier pour enregistrer ou communiquer de l'information ou des transactions ».

Bien qu'il n'y ait pas de lois spécifiques qui touchent les NTSC au fédéral, certains textes normatifs ont été élaborés à cet égard.

Par exemple, le Commissariat à la protection de la vie privée du Canada a établi quatre critères afin de déterminer les répercussions des technologies biométriques et d'autres mesures de sécurité sur la vie privée[91] :

1. La mesure est manifestement nécessaire pour répondre à certains besoins ;
2. Tout indique que la mesure sera probablement efficace pour satisfaire les besoins à l'origine du déploiement proposé ;
3. L'ingérence dans la vie privée est proportionnelle à l'avantage en matière de sécurité ;
4. Il peut être montré qu'aucune autre mesure comportant une ingérence moindre dans la vie privée ne permettrait d'atteindre les mêmes résultats.

De plus, le Commissariat à la protection de la vie privée du Canada a tracé des lignes directrices concernant le recours, par les forces policières et les autorités chargées de l'application de la loi, à la surveillance vidéo dans les lieux publics[92].

La protection de la vie privée et des renseignements personnels à l'échelle régionale et internationale

Certains textes internationaux, de même que certains textes relatifs à l'Europe et aux États-Unis, méritent aussi d'être mentionnés.

Sur le plan international, il faut souligner l'existence de la Déclaration universelle des droits de l'homme de l'Organisation des Nations Unies (ONU), qui affirme l'importance du droit à la vie privée (à l'article 12). L'Organisation de coopération et de développement économiques (OCDE) a également produit en 1980 des lignes directrices s'intitulant *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel.*

Sur le plan européen, l'article 8 de la Convention européenne des droits de l'homme traite spécifiquement du droit au respect de la vie privée et familiale. La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel de 1981 et la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données réaffirment l'importance du droit à la vie privée et se concentrent sur l'encadrement de la collecte, l'utilisation, la conservation et la communication de renseignements personnels.

91. « La biométrie faciale est-elle à la hauteur ? Le Bureau des passeports du Canada répond à la question », *III@L'OEUVRE*, été 2004, p. 21.
92. Voir l'annexe 2.

La Directive en quelques mots...

Afin de lever les obstacles à la libre circulation des données sans diminuer la protection des données personnelles, la directive 95/46/CE (directive sur la protection des données) fut mise au point pour harmoniser les dispositions nationales dans ce domaine. Il en résulte que les données personnelles de tous les citoyens disposeront d'une protection équivalente dans l'ensemble de l'Union. Les quinze États membres de l'UE étaient tenus d'aligner leur législation nationale sur les dispositions de la directive d'ici au 24 octobre 1998.

Une directive est un acte législatif européen dont les États membres sont destinataires. Une fois cette législation adoptée au niveau européen, chaque État membre doit en assurer la transposition efficace dans son système juridique. [...]

La directive sur la protection des données s'applique à « toute opération ou ensemble d'opérations appliquées à des données à caractère personnel », désignées comme « traitement des données ». Ces opérations comprennent la collecte des données personnelles, leur conservation, leur diffusion, etc. La directive s'applique aux données traitées par des moyens automatisés (par exemple une base de données informatique de clients) ainsi qu'aux données faisant partie ou destinées à faire partie de fichiers non automatisés dans lesquels celles-ci sont accessibles suivant des critères spécifiques (par exemple les fichiers papiers traditionnels, tels qu'un fichier sur cartes dans lequel les données de la clientèle sont rangées par ordre alphabétique)[93].

En ce qui a trait à la biométrie, il convient de souligner l'initiative de l'International Biometric Industry Association qui a élaboré un instrument d'autorégulation. Cependant, un seul des cinq principes énoncés porte sur la protection de la population, les autres relevant de l'éthique des affaires et des bonnes pratiques commerciales :

> *Members believe that biometric technologies should be used solely for legal, ethical, and nondiscriminatory purposes. They are therefore committed to the highest standards of systems integrity and database security in order to deter identity theft, protect personal privacy, and ensure equal rights under the law in all biometric applications*[94].

93. COMMISSION EUROPÉENNE, *Protection des données dans l'Union européenne. Dialogue avec les citoyens et les entreprises*, guide sur la protection des données, Belgique, 2000, p. 4.

94. INTERNATIONAL BIOMETRIC INDUSTRY ASSOCIATION, *IBIA Statement of Principles and Code of Ethics*, 23 octobre 2000, [http://www.ibia.org/aboutibia/ethics.asp].

Chapitre 2
Les nouvelles technologies de surveillance et de contrôle : un tour d'horizon

Devant cette insécurité provoquée notamment par les récents attentats terroristes, des États ont réagi en mettant en place un processus de sécurisation passant par l'utilisation de nouvelles technologies de surveillance et de contrôle (NTSC) : la biométrie, la vidéosurveillance et l'identification par radiofréquence (IRF) comptent parmi celles-ci. Ces technologies sont déjà en application, mais à des degrés très différents. Par le présent tour d'horizon, la Commission désire donner au lecteur une meilleure compréhension des technologies afin qu'il soit en mesure de saisir les répercussions de leurs implantations sur le plan éthique.

Les systèmes biométriques : obéir au doigt et à l'œil ?

Mis à part l'utilisation des empreintes digitales dans le système judiciaire et, plus récemment, celle de lecteurs de la main comme moyens de contrôle de l'accès à certains édifices, les technologies biométriques sont généralement peu connues de la population. Qu'elles soient cependant mal connues ou peu connues, ces technologies n'en suscitent pas moins « fascination et inquiétude[95] », pour reprendre les mots de Jennifer Stoddart, présidente de la Commission d'accès à l'information (CAI) jusqu'en 2004. La Commission de l'éthique de la science et de la technologie décrit le fonctionnement et l'objet des systèmes biométriques dans les paragraphes qui suivent.

Quelques définitions utiles

En français, il existe différentes acceptions du terme « biométrie »[96]. Sous l'influence de l'anglais, et dans le domaine de la sécurité, le terme en est venu à désigner les « techniques permettant d'identifier une personne à partir de l'un ou plusieurs de ses caractères biologiques ou comportementaux[97] ».

Un système biométrique devient donc une application technologique « permettant l'identification automatique ou l'éligibilité [*sic*] d'une personne à se voir reconnaître certains droits ou services (notamment l'accès) basés sur la reconnaissance de particularités physiques (empreintes digitales, iris de l'œil, contour de la main...), de traces (ADN, sang, odeurs) ou d'éléments comportementaux (signature, démarche)[98] ».

Les données biométriques constituent les informations à caractère morphologique, biologique ou comportemental propres à une personne. Il y a quelques années à peine, la technologie permettant de mesurer une diversité de caractéristiques biométriques et de les utiliser à des fins d'identification était relativement peu développée – hormis la technologie relative aux empreintes digitales, la plus courante et la plus ancienne. Aujourd'hui, aucun caractère biométrique ne semble exclu *a priori* et n'importe quelle caractéristique personnelle semble pouvoir se prêter à une mesure (à un niveau de fiabilité variable, cependant) par la technologie biométrique : différentes parties du corps, la voix, le geste, l'odeur, la chaleur corporelle, etc.

95. Jennifer STODDART, « Des technologies de surveillance sous surveillance », Discours [en ligne], septembre 2001, [http://www.cai.gouv.qc.ca/05_communiques_et_discours/discours_24_09_01.html].

96. Dont, notamment, « science des variations biologiques, des phénomènes qui s'y rattachent et des problèmes qui en découlent », Eugène SCHREIDER, article sur la biométrie dans l'*Encyclopedia Universalis*.

97. OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, *Les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre*, Christian CABAL, député, Sénat, Assemblée nationale (France), juin 2003, p. 7.

98. Définition de la Commission nationale de l'informatique et des libertés (CNIL – France), rapportée dans OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, *op. cit.*, note 6, p. 8.

Le rôle des technologies de l'information est fondamental dans le traitement (notamment la numérisation de l'information « physique » qui est recueillie) et l'analyse des données, ainsi que dans l'interface qu'elles permettent d'établir avec les bases de données de toutes sortes sur les personnes (données d'identification personnelle, financières, médicales, etc.). Ces technologies permettent aux systèmes biométriques d'effectuer des traitements de masse quasi instantanément et avec un taux de fiabilité qui ne peut qu'augmenter dans les années à venir – tout comme leur « invisibilité », d'ailleurs, du fait qu'ils s'intègrent de plus en plus dans notre environnement.

Dans le domaine de la sécurité, il convient de mentionner que la biométrie est utilisée à deux fins principales : l'identification d'une personne et l'authentification d'une personne (ou la vérification de son identité). Avec le développement d'applications de masse, cependant – qui rendront possible la constitution de bases de données biométriques concernant des millions de personnes –, une troisième utilisation, le « dépistage » (ou « *screening* »), pourrait prendre de l'ampleur.

Dans le contexte de l'identification, la question suivante est posée : Qui est cette personne ? et donne lieu à une recherche de type « un à plusieurs » dans une base de données, centralisée ou intégrée au système, souvent dans un contexte judiciaire – par exemple à partir d'empreintes digitales, avec pour objectif de découvrir l'identité d'une personne (victime d'un crime ou ayant laissé des traces sur le lieu d'un crime).

Dans le contexte de l'authentification ou de la validation d'identité, la question Cette personne est-elle bien celle qu'elle prétend être ? donne lieu à une recherche de type « un à un ». Il doit alors y avoir concordance de l'information fournie avec une information déjà colligée sur un support quelconque (informatisé ou non)[99], comme dans le cas de droits d'accès à des installations matérielles à partir de la lecture de la main, de l'iris ou d'empreintes digitales. Ce type de recherche « un à un » ne permet pas la traçabilité et le profilage des personnes, c'est-à-dire qu'il ne permet pas de cibler des personnes ou des groupes à partir de certaines caractéristiques biométriques. L'identité d'une personne est validée ou confirmée au moment où cette personne requiert un service ou un accès préalablement autorisé.

La distinction entre ces deux finalités est importante car, selon la caractéristique biométrique retenue et son mode de stockage (information centralisée dans une base de données ou inscrite sur un support informatique ou non), mais aussi selon les objectifs poursuivis, le risque pour la protection de la vie privée et des renseignements personnels pourra différer.

En ce qui a trait au dépistage, la question posée pourrait être : Où est cette personne ? Le procédé permet alors notamment de confronter les données contenues dans une liste de personnes sous surveillance (criminels, terroristes, activistes, etc.) avec le contenu de bases de données biométriques d'une vaste population (les photos numérisées des passeports, par exemple, ou obtenues à partir de caméras de surveillance) afin d'en tirer toute information pouvant contribuer à appréhender un criminel ou un suspect[100].

Les finalités associées à l'utilisation des données biométriques

Les systèmes biométriques sont mis en place afin de répondre à des finalités bien précises[101]. En voici quelques exemples :

- la prévention du crime (identification de criminels, de terroristes, etc.) ;
- la prévention de l'usage frauduleux de documents ;
- le renforcement de la fiabilité des titres délivrés ;
- le contrôle de l'accès à des locaux et à des sites physiques ;
- le contrôle de l'accès à de l'équipement informatique (matériels et logiciels) ;
- le contrôle de l'accès à des applications de chiffrement ;
- la surveillance du travail des responsables de la sécurité (surveillance continue en temps réel).

99. Information tirée, entre autres, de CITOYENNETÉ ET IMMIGRATION CANADA, « Biométrie : incidences et applications pour la citoyenneté et l'immigration », document d'information, Forum tenu les 7 et 8 octobre 2003, Ottawa, Canada, p. 2.

100. INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES, *Biometrics at the Frontiers : Assessing the Impact on Society*, Technical Report Series, 2005, p. 39-40.

101. Bernard DIONNE et Evelyne RACETTE, « La biométrie : présentation à la Commission de l'éthique de la science et de la technologie », mars 2004 (manuscrit).

Les différentes technologies actuelles et en développement et leur mode de fonctionnement

Les systèmes biométriques peuvent être classés en fonction de trois catégories de données particulières à une personne[102] :

- *Les données morphologiques ou physiologiques*

  Cette catégorie s'appuie sur l'identification de traits physiques qui sont uniques et permanents chez une même personne. Les éléments retenus à des fins d'identification biométrique sont généralement reconnus pour leur stabilité et ils ne subissent pas autant les effets du stress ou du vieillissement, par exemple, que les traits comportementaux[103]. Reste que des facteurs comme l'environnement et certains états passagers (rhume, transpiration) peuvent altérer la fiabilité de la lecture. La biométrie morphologique ou physiologique regroupe notamment la reconnaissance des empreintes digitales, de la forme de la main, de la forme du visage, de la voix, de la rétine (dessin du réseau veineux du fond de l'œil), de l'iris de l'œil et la thermographie.

- *Les données comportementales*

  Cette catégorie est fondée sur l'analyse d'actions répétitives et usuelles du comportement humain. La prémisse à ce type d'analyse est que le comportement de chacun constitue une signature personnelle. Certains mouvements chez une personne lui sont propres et peuvent confirmer son identité. La biométrie comportementale comprend la dynamique de la signature, de la frappe au clavier d'ordinateur, la façon de marcher, etc.

- *Les données biologiques*

  Cette catégorie a recours à l'analyse de traces biologiques, comme l'empreinte génétique (ADN), l'odeur, la salive, l'urine, etc.

En matière de fonctionnement, tous les systèmes biométriques fonctionnent en deux temps et comportent deux processus :

- l'enregistrement d'un utilisateur ;
- le contrôle d'un utilisateur.

Ces deux processus comprennent cinq étapes essentielles au bon déroulement de l'opération[104] :

1) la saisie de l'information à analyser – lecture de certaines caractéristiques physiologiques, comportementales ou biologiques d'une personne au moyen d'un terminal de capture biométrique (ou capteur biométrique) ;

2) le traitement de l'information – transformation de l'information en données numériques ;

3) la création d'un fichier « signature » et son enregistrement – utilisation des données numériques pour créer un modèle ou gabarit qui représente la donnée biométrique captée, c'est-à-dire la signature qui sera conservée sur un support portable (puce ou autre) ou dans une base de données et utilisée pour comparaison ;

4) la comparaison – comparaison des caractéristiques biométriques d'une personne soumise à contrôle (volontairement ou à son insu) sont comparées à la « signature » mémorisée ; l'identité de l'utilisateur correspond à l'identité proclamée ou recherchée ou elle ne correspond pas ;

102. Bernard DIONNE et Evelyne RACETTE, *op. cit.* Il convient toutefois de souligner qu'il peut exister des systèmes de surveillance qui ne comportent pas de phases d'enregistrement tout en permettant une analyse de comportements à risques (surveillance vidéo d'un stationnement, par exemple, et repérage d'un voleur potentiel à partir de ses agissements).

103. Dans un rapport de la LONDON SCHOOL OF ECONOMICS & POLITICAL SCIENCE, cette assertion est cependant nuancée pour souligner les effets du vieillissement, non seulement sur la transformation des données biométriques, mais aussi dans l'utilisation des moyens techniques mis en place pour la lecture de ces données (tremblements, arthrite, cataractes, paupières tombantes, etc.). Le rapport souligne aussi qu'aucune étude scientifique n'a été réalisée sur la stabilité des caractéristiques biométriques dans le temps. Voir LONDON SCHOOL OF ECONOMICS & POLITICAL SCIENCE, *The Identity Project. An Assessment of the UK Identity Cards Bill & Its Implications*, Department of Information Systems, 27 juin 2005, p. 170-175.

104. Bernard DIONNE et Evelyne RACETTE, *op. cit.*, et COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *La biométrie au Québec : les enjeux*, Document d'analyse, juillet 2002, p. 8 et 9.

5) la décision – décision par l'opérateur du système ou le système informatisé à savoir si l'identité de l'utilisateur correspond ou non à l'identité proclamée (authentification) ou recherchée (identification).

Les techniques biométriques s'appuient sur le principe qu'il est possible de relier une donnée à une personne. Ce principe couvre l'unicité du caractère biométrique choisi et l'unicité de la mesure ou de la représentation graphique de ce caractère, l'une comme l'autre étant propres à une seule et même personne. La biométrie repose sur des méthodes statistiques destinées à déterminer la probabilité que deux personnes présentent la même donnée (généralement très faible pour la plupart des données biométriques actuelles sauf pour les jumeaux identiques, nulle pour l'iris – les deux iris d'une même personne sont d'ailleurs différents).

Toutes les études insistent sur le caractère crucial de la phase d'enregistrement. Plus les personnes collaborent au processus, plus les systèmes biométriques sont efficaces.

Les atouts des technologies biométriques

Comme le souligne la Commission de l'accès à l'information :

> *la biométrie est présentée au grand public comme un remède universel propre à terrasser plusieurs maux : terrorisme, fraude, vol d'identité et atteinte à la vie privée, pour n'en citer que quelques-uns. Aux employeurs elle est présentée comme une solution au vol de temps par les travailleurs, comme un moyen facile de produire les données de base servant au calcul de la paye. Aux utilisateurs elle est présentée comme un moyen confortable de s'identifier : plus de cartes qu'on égare et de mots de passe qu'on oublie*[107].

Dans son rapport présenté au Sénat français, le député Christian Cabal note que les systèmes biométriques se révèlent un instrument efficace de lutte contre la fraude – fraude électronique et usage frauduleux de documents (à l'échelle mondiale, des milliards de dollars pour les cartes de crédit), pour assurer la sécurité des échanges financiers et commerciaux, l'accès légitime aux services gouvernementaux, et pour contrer le vol d'identité sous toutes ses formes[108].

Habituellement, la biométrie est présentée comme une technologie permettant d'éradiquer, du moins en partie, le phénomène du vol d'identité. Les pièces d'identité, les cartes de crédit et les titres donnant accès à des services sociaux, par exemple, sont des documents précieux qui font régulièrement l'objet de fraude. En théorie, l'insertion de données biométriques dans ces documents permettrait donc de limiter les incidences de fraude, car le malfaiteur serait confronté à un défi de taille : modifier les données biométriques contenues dans le document pour les conformer aux siennes ou, inversement, modifier ces dernières afin de les conformer à celles qui se trouvent dans le document. La biométrie semble être en mesure de donner des maux de tête aux futurs fraudeurs, surtout qu'elle peut être utilisée pour chiffrer des données personnelles.

Cela dit, contrairement au vol d'identité traditionnel, le vol d'identité biométrique porte davantage à conséquence. De fait, le vol d'identité serait alors très difficile à prouver et la réhabilitation de l'association entre une donnée biométrique et la véritable personne de qui celle-ci émane pourrait s'avérer tout aussi complexe. La CAI du Québec précise que :

> *La stabilité des mesures ou des caractéristiques biométriques comme identifiant pourrait devenir un véritable cauchemar pour les personnes victimes de vol d'identité. Même si ces personnes réussissaient à prouver leur innocence, leur identifiant intime serait compromis à tout jamais [...]. De même un individu malveillant qui réussirait à accoler ses données biométriques à l'identité d'une autre personne pourrait causer un tort immense et difficilement réparable à la personne victime d'un tel stratagème*[107].

Dans l'ensemble, les technologies biométriques sont présentées par leurs promoteurs comme des mécanismes de protection pouvant garantir qu'en aucun cas les caractéristiques personnelles qui sont analysées ne peuvent être utilisées à d'autres fins que celles recherchées par le système d'information, pour les raisons suivantes[108] :

- unicité de la donnée biométrique ;
- mécanisme de chiffrement fort, pour assurer la confidentialité ;

105. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *La biométrie au Québec : les enjeux*, Document d'analyse, juillet 2002, p. 23.
106. OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, *op. cit.*, p. 46-51.
107. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *La biométrie au Québec : les enjeux*, Document d'analyse, juillet 2002.
108. Bernard DIONNE et Evelyne RACETTE, *op. cit.*

- fonctions de traitement à sens unique, pour assurer l'anonymat. Cette fonction est un processus d'enregistrement qui ne permet pas la régénération de l'image du doigt, du visage, de la main, du code génétique, de la couleur, etc. Ainsi, l'analyse du fichier signature seul ne permet pas d'identifier la personne concernée (ni de découvrir une pathologie quelconque);
- mécanisme de signature des fichiers références, pour garantir leur authenticité et leur intégrité;
- mécanismes pour contrer la falsification.

Les avantages suivants peuvent être avancés en matière d'utilisation des données biométriques[109]:

- améliorer la sécurité des personnes (ou réduire la détresse des victimes);
- protéger efficacement les données personnelles;
- lutter efficacement contre la fraude, parce que chaque personne possède ses propres caractéristiques physiques, comportementales ou biologiques qui ne peuvent être ni perdues, ni volées;
- contrer la prolifération des mots de passe et la nécessité de les mémoriser – d'autant plus que les gens ont souvent tendance à les inscrire quelque part ou à utiliser des mots de passe ou des NIP faciles à deviner (date de naissance, nom d'un enfant, etc.);
- contrer la supercherie – une pratique par laquelle les pirates informatiques se font passer pour un spécialiste, un technicien ou une personne en autorité pour subtiliser l'identifiant personnel ou le mot de passe d'une personne.

Les failles des technologies biométriques

En ce qui a trait aux failles (ou aux inconvénients) des technologies biométriques, les arguments soulevés concernent davantage les systèmes d'information et sont liés[110]:

- aux menaces de la collecte non nécessaire;
- au traitement (risque de restreindre les libertés individuelles);
- à la communication (non autorisée) des informations;
- à l'interconnexion des bases de données facilitée par le recours à un identifiant unique (finalité);
- au coût.

Par rapport aux caractéristiques de la biométrie, les inconvénients les plus appréhendés sont les suivants[111]:

- information intrinsèquement liée à la personne (possibilité de découvrir des maladies);
- nécessité de se soumettre physiquement au processus de vérification (méthode considérée intrusive);
- difficulté de se défaire de ses caractéristiques biométriques (unicité de la donnée) et difficulté d'apporter la preuve que la personne n'a pas commis les actes qui lui sont imputés en cas de falsification (faux élément biométrique) ou d'usurpation (vol du fichier de signature) d'identité;
- comparaison biométrique qui apporte un taux d'incertitude sur la validité du client accepté (fausse acceptation) ou refusé (faux rejet), au contraire de l'utilisation des systèmes traditionnels d'authentification, tels le mot de passe ou le jeton, qui produisent une réponse sûre à 100 % (vrai ou faux). La difficulté est de trouver un compromis acceptable entre l'exigence de sécurité (haut taux de faux rejets) et la nécessité d'un système plus « convivial » (haut taux de fausses acceptations).

L'avantage de l'unicité de la donnée biométrique peut cependant devenir une vulnérabilité. Contrairement à un mot de passe, à un certificat électronique ou à une clé de chiffrement, il est difficile de modifier une donnée biométrique recueillie pour identifier une personne – une fois cette donnée volée ou usurpée, la personne à qui celle-ci renvoie véritablement peut difficilement faire la preuve du vol. En outre, les techniques biométriques peuvent elles aussi être trompées par des artifices, même lorsqu'il y a présence de mécanismes pour contrer la falsification. Et plus les mécanismes de contre-mesure se développeront, plus les techniques de falsification gagneront en sophistication.

109. *Ibid.*
110. *Ibid.*
111. *Ibid.*

Pour résumer quelque peu l'information apportée sur les données biométriques dans la présente section, le tableau qui suit fournit une synthèse des principaux critères relatifs aux différentes technologies mises au point ou à venir, tels que rapportés par l'Office d'évaluation des choix scientifiques et technologiques (France) et par l'Organisation de coopération et de développement économiques (OCDE).

Il est important de noter qu'il s'agit d'un domaine qui évolue rapidement et que les « performances » mentionnées dans le tableau ont pu s'améliorer depuis le moment de l'évaluation d'une technique particulière. En outre, de nombreuses nuances pourraient sans doute être ajoutées aux évaluations qui sont rapportées dans ce tableau, notamment au regard de la fiabilité.

Tableau synthèse sur les données biométriques

Biométrie[112]	Robustesse[113]	Unicité[114]	Fiabilité[115]	Potentiel[116]	Acceptabilité[117]	Coût	Applications
Empreintes digitales	Moyenne-haute	Haute	Très haute	Haut	Basse-moyenne	Très faible-moyen	Voyageurs, permis de conduire, domaine judiciaire
Géométrie de la main	Moyenne-haute	Haute	Haute	Moyen-haut	Moyenne-haute	Moyen	Contrôles d'accès, voyageurs
Géométrie des doigts	Moyenne-haute	n. d.	Moyenne-haute	n. d.	Moyenne-haute	Moyen	Contrôles d'accès, détenteurs de billets dans les parcs d'amusement
Reconnaissance faciale	Moyenne	Haute	Basse	Moyen	Haute	Moyen	Casinos, voyageurs
Iris	Haute	Très haute	Haute	Haut-très haut	Moyenne-haute	Très élevé	Prisons, contrôles d'accès, voyageurs
Rétine	Haute	Très haute	Haute	n. d.	Basse	Élevé	Contrôles d'accès, voyageurs
Signature	Basse-moyenne	Moyenne	Basse	Bas-moyen	Moyenne-haute	Faible	Applications à faible niveau de sécurité, applications comportant déjà une signature
Voix	Moyenne	Moyenne-haute	Moyenne-haute	Moyen-haut	Haute	Faible	Applications à faible niveau de sécurité, authentification téléphonique
Odeur	Niveau inconnu	Niveau inconnu	Bas	Niveau inconnu	n. d.	n. d.	n. d.
Oreille	Niveau inconnu	Niveau inconnu	Bas	Niveau inconnu	n. d.	n. d.	n. d.
Imagerie thermique	Niveau inconnu	Niveau inconnu	Bas	Niveau inconnu	n. d.	n. d.	n. d.
Frappe sur clavier	Niveau inconnu	Niveau inconnu	Bas	Niveau inconnu	n. d.	n. d.	n. d.

Sources : OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES (France)[118] et OCDE[119].

112. Parce qu'elle ne peut être réalisée sur-le-champ, l'analyse de l'ADN ne fait pas partie des données biométriques de ce tableau. Toutefois, l'évolution de la technologie devrait pallier cette contrainte à plus ou moins court terme. La reconnaissance de la démarche est également absente du tableau, les sources utilisées n'en ayant pas fait l'évaluation.

113. La robustesse indique le degré de stabilité de l'élément biométrique pendant une période donnée ; voir OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, *op. cit.*, p. 37.

114. L'unicité indique la capacité de discrimination d'un individu par rapport à un autre ; voir *Ibid.*

115. La fiabilité considère les taux d'erreur : fausses acceptations et faux rejets.

116. Sur la base de la robustesse, de l'unicité et de la fiabilité, le potentiel biométrique permet d'apprécier la sécurité qu'apporte l'élément biométrique utilisé ; voir OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, *op. cit.*, p. 37.

117. Les données concernant l'acceptabilité des personnes relativement à la technique mentionnée, le coût et les applications sont tirées de l'OEDC (OCDE), *Biometric-based Technologies*, Working Party on Information Security and Privacy, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy, Paris, 28 avril 2004.

118. OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, *op. cit.*, p. 38 et 39.

119. *Ibid.*, p. 36.

Enfin, une société américaine – l'International Biometric Group – propose le classement suivant de huit techniques biométriques[120] :

- « des techniques les moins "intrusives"[121] aux plus "intrusives" : la voix, la frappe sur le clavier, la signature, la main, la face, l'empreinte digitale, l'iris et enfin la rétine ;
- des techniques les plus fiables aux moins fiables : l'iris, la rétine, l'empreinte digitale, la face, la main, la voix et enfin, à un niveau équivalent, la frappe sur le clavier et la signature ;
- des techniques les moins chères aux plus chères : la frappe sur le clavier, la voix, la signature, l'empreinte digitale, la face, la main, la rétine et enfin l'iris ;
- des techniques les plus faciles d'utilisation aux plus difficiles : la face, la signature, l'iris, la frappe sur le clavier, la voix, l'empreinte digitale, la main et enfin la rétine. »

Le marché de la biométrie

Selon Citoyenneté et Immigration Canada, les recettes de l'industrie biométrique totalisaient 601 millions de dollars américains en 2002, pour une estimation de 4 milliards d'ici à 2007, en raison de l'intérêt croissant des gouvernements et des firmes pour cette technologie[122]. Pour 2007, l'estimation actuelle est légèrement inférieure, soit à 3 milliards de dollars. Une croissance soutenue est prévue de telle sorte qu'en 2012 l'industrie de la biométrie générerait des revenus totalisant 7,4 milliards de dollars américains[123].

En août 2004, Industrie Canada estimait qu'environ 200 entreprises se partagent les trois grands créneaux des technologies de la sécurité au Canada : authentification, biométrie et cyberprotection, dont le tiers dans la grande région montréalaise[124]. Ce marché est en pleine expansion et peut exercer une pression sur la prise de décision relative à l'utilisation des données biométriques à des fins de sécurité. Bien que la Commission n'ait pas exploré cet aspect de la question de façon exhaustive, elle souhaite aborder le sujet pour en saisir les incidences éventuelles sur le plan du questionnement éthique.

Le marché est reconnu pour être difficile à appréhender dans sa globalité[125], car il est fragmenté en fonction des données biométriques privilégiées et du type de système développé (grands systèmes d'identification portant sur les empreintes digitales, par exemple, qui représentent environ 25 % du marché international et petits terminaux ou capteurs biométriques destinés à différentes données biométriques). Sur le plan international, le secteur est largement dominé par les sociétés américaines et par la technologie relative aux empreintes digitales.

Les objectifs de modernisation et d'harmonisation des instruments d'identification judiciaire afin d'assurer une meilleure coopération entre les États, mais aussi le fait que plusieurs gouvernements envisagent de doter leurs citoyens et résidents de titres biométriques, font en sorte que l'industrie de la biométrie a le vent dans les voiles. Certains estiment, cependant, que le besoin de normalisation du secteur pourra jouer un rôle dans la compétition[126]. La normalisation (ou standardisation) a pour but de faciliter les échanges et l'interopérabilité (accès à de l'information ou à des bases de données par différents systèmes) des systèmes biométriques – et donc la comparaison de données, d'éviter que les utilisateurs soient dépendants de systèmes propriétaires, d'harmoniser les méthodes et les principes d'évaluation des performances et de déterminer quels sont les outils nécessaires pour assurer la sécurité des frontières[127]. Les enjeux de la normalisation sont à la fois politiques et économiques. À ce sujet, un questionnement s'impose : les pays disposant des meilleures technologies seront-ils à même d'imposer leurs propres exigences en matière de protection des renseignements personnels et de respect de la vie privée ?

120. *Ibid.*, p. 40.

121. Précisons qu'il s'agit ici de l'intrusion sur le plan physiologique et non en matière de collecte de renseignements personnels.

122. CITOYENNETÉ ET IMMIGRATION CANADA, « Biométrie : incidences et applications pour la citoyenneté et l'immigration », document d'information, Forum tenu les 7 et 8 octobre 2003, Ottawa, Canada, p. 6.

123. INTERNATIONAL BIOMETRIC GROUP, *Biometrics Market and Industry Report 2007-2012*.

124. Voir INDUSTRIE CANADA, « L'industrie canadienne de la sécurité : centres d'activité ».

125. Voir particulièrement OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, *op. cit.*, p. 49.

126. *Ibid.*, p. 48.

127. *Ibid.*, p. 52.

L'intérêt de la population[128]

Les deux plus récents efforts afin de mesurer l'intérêt de la population pour la biométrie sont les suivants : la consultation de Citoyenneté et Immigration Canada en 2002 et 2003 et un sondage TNS/TRUSTe en 2005.

Un sondage téléphonique a été réalisé auprès de la population canadienne en novembre 2002 sur la possibilité d'instaurer une carte d'identité nationale avec des données biométriques. En février 2003, seize groupes de consultation composés de citoyens et de résidents permanents ont eu à se prononcer sur le sujet. En octobre 2003, Citoyenneté et Immigration Canada tenait un forum public sur les incidences et les applications de la biométrie pour la citoyenneté et l'immigration, et en publiait les actes par la suite.

Le sondage révèle que les Canadiens sont majoritairement favorables à la mise au point d'une carte d'identité munie d'un identificateur biométrique comme les empreintes digitales ou la numérisation oculaire afin de réduire l'utilisation frauduleuse des documents d'identité (73 %), des passeports ou de différents documents d'accessibilité aux programmes gouvernementaux (80 %). Malgré tout, certains croient que l'utilisation de cette technologie irait à l'encontre des valeurs de liberté et d'équité (36 %) et nuirait à la protection des renseignements personnels (53 %).

Dans le cas des groupes de consultation, les participants en faveur de l'instauration d'une carte avec données biométriques y voyaient les avantages suivants : augmentation de la sécurité, amélioration du contrôle de l'immigration et des frontières, réduction de l'utilisation frauduleuse des programmes gouvernementaux, leadership pour le Canada en matière de technologie d'identification. Les opposants soulevaient les points suivants : des préoccupations à l'égard des coûts, de l'atteinte à la vie privée et à la liberté et de la gestion du système, des résistances à l'égard d'un programme de sécurité dirigé par les États-Unis.

Des mémoires sur le sujet ont également été présentés au Comité permanent de la citoyenneté et de l'immigration. Ils attestent clairement que les Canadiens veulent être assurés que la biométrie serait « utilisée conformément aux principes de protection de la vie privée généralement reconnus et conformément aux valeurs canadiennes[129] ». Certains craignent le caractère intrinsèquement intrusif de la biométrie, qui peut toucher des aspects intimes de la personne, comme son état de santé – lecture de l'iris et diabète ou hypertension, empreintes digitales et syndromes de Down ou de Turner –, ainsi que ses répercussions possibles sur les libertés fondamentales. La création d'une « infrastructure de surveillance » fait également partie des préoccupations mentionnées, et toute intrusion de l'État est perçue « comme une action répréhensible, une invasion de l'espace privé, et l'antithèse des principes d'une société libre et ouverte où les valeurs sont tout aussi importantes que l'avancement des technologies[130] ».

La tenue du forum visait les objectifs suivants :

- *explorer la biométrie comme une technologie puissante susceptible de faciliter l'atteinte de futurs objectifs stratégiques importants ;*
- *améliorer et élargir le débat actuel sur les aspects techniques et sociaux reliés à l'utilisation de la biométrie à l'appui de l'intégrité des documents et de la vérification de l'identité ;*
- *comparer les avantages et les inconvénients d'une approche globale de la « carte d'identité nationale » par rapport à une stratégie plus progressive qui consisterait à améliorer les nombreux documents d'identité existants ;*
- *engager un dialogue sur les questions importantes avant la mise en œuvre de toute politique*[131].

Choisis pour apporter le plus grand nombre possible de points de vue, de positions et d'opinions sur l'identité, le respect de la vie privée et d'autres questions connexes, les participants ont conclu les débats en reconnaissant qu'il fallait une solution « typiquement canadienne » au problème des documents d'identité et une collaboration avec les provinces et les territoires pour élaborer une approche nationale en la matière.

128. L'information est tirée de CITOYENNETÉ ET IMMIGRATION CANADA, *Biométrie : incidences et applications pour la citoyenneté et l'immigration*, document d'information, Forum tenu les 7 et 8 octobre 2003, Ottawa, Canada, p. 10.

129. *Ibid.*, p. 16.

130. *Ibid.*

131. CITOYENNETÉ ET IMMIGRATION CANADA, *Biométrie : incidences et applications pour la citoyenneté et l'immigration*, Actes du forum tenu à Ottawa les 7 et 8 octobre 2003, p. 2.

Quant au sondage TNS/TRUSTe de 2005, il apporte les résultats suivants : 85 % des Canadiens se disent favorables à l'introduction d'identifiants biométriques dans le passeport canadien ; cet appui est aussi fort pour l'introduction de tels identifiants dans d'autres documents d'identité comme le permis de conduire, les cartes d'assurance sociale et d'assurance maladie[132]. De plus, plus de huit Canadiens sur dix pensent « que les empreintes digitales représentent la forme la plus acceptable d'identité biométrique, suivies de la reconnaissance de l'iris[133] » (à 67 %). Sur le plan des préoccupations des Canadiens sur le sujet, le coût d'implantation, les risques d'usages abusifs de l'information par le gouvernement figurent au nombre des principales inquiétudes.

La vidéosurveillance : l'œil omniprésent

La vidéosurveillance consiste en la surveillance à distance de lieux publics ou privés, à l'aide de caméras le plus souvent motorisées, qui transmettent les images saisies à un équipement de contrôle qui les reproduit sur un écran. Contrairement aux autres technologies de surveillance et de contrôle décrites dans le présent avis, la vidéosurveillance n'est pas à proprement parler une technologie nouvelle. Deux raisons ont particulièrement motivé la Commission à traiter de la question. Tout d'abord, des avancées technologiques récentes ont élargi l'éventail des possibilités qu'offre la surveillance par caméra. Outre la miniaturisation et le camouflage des caméras (permettant plus facilement de filmer des personnes à leur insu) et la numérisation des images (facilitant le stockage et l'analyse des données), il faut également mentionner le développement de logiciels dits intelligents dont la fonction principale consiste à repérer les personnes dont le comportement dévie de la norme. Par ailleurs, le couplage maintenant possible avec d'autres NTSC apparaît comme une autre raison d'inclure la vidéosurveillance dans l'analyse. De fait, la numérisation des images permet la reconnaissance faciale des personnes filmées et la comparaison avec des données biométriques préalablement recueillies.

L'ampleur du phénomène de la vidéosurveillance est difficile à évaluer. Des affichettes apposées à l'entrée de presque tous les bâtiments très fréquentés, comme les centres commerciaux et les édifices gouvernementaux, signalent la présence de caméras de surveillance. Force est donc de constater que les Québécois sont régulièrement filmés. Le travail de la CAI, qui a tenu en 2003 une vaste consultation publique sur la vidéosurveillance, a permis de mieux connaître l'état des lieux. Dans le *Bilan* de cette consultation, le commissaire Michel Laporte énonce certains constats qui caractérisent la situation québécoise :

- *La vidéosurveillance est utilisée depuis plus de 28 ans par certains organismes publics et majoritairement opérée sous leur responsabilité directe ;*
- *L'utilisation des caméras de surveillance n'est donc pas un phénomène récent ni en décroissance ;*
- *Les organismes publics ont manifesté un intérêt évident pour accroître l'utilisation de la vidéosurveillance ;*
- *Les caméras de surveillance installées dans les rues et parcs ou places publiques ne sont l'apanage que de certaines villes précises ;* [...]
- *Les données touchant certains organismes pouvant potentiellement être d'importants utilisateurs de la vidéosurveillance mériteraient d'être mieux documentées, connues et approfondies, et ce, aux fins d'enrichir l'état des débats et de nos connaissances ;*
- *L'utilisation de la vidéosurveillance par les entreprises privées au Québec semble peu documentée*[134].

De ces remarques, deux conclusions peuvent être dégagées : 1) l'étendue de l'utilisation des caméras de surveillance est mal connue ; 2) cette étendue serait croissante. C'est peut-être pourquoi plusieurs instances, à l'instar de la CAI, se sont récemment penchées sur la question telles que le Commissariat à la protection de la vie privée du Canada[135] et aux organismes responsables de la protection de la vie privée et des renseignements

132. « Les Canadiens et les Américains appuient l'application de la technologie biométrique pour les passeports et les permis de conduire – sondage », communiqué de presse, Toronto, 2 août 2005.

133. *Ibid.*

134. Michel LAPORTE, *op. cit.*, p. 19.

135. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Lignes directrices du Commissariat à la protection de la vie privée du Canada concernant le recours, par les forces policières et les autorités chargées de l'application de la loi, à la surveillance vidéo dans les lieux publics*, mars 2006, [http://www.privcom.gc.ca/information/guide/vs_060301_f.asp].

personnels de l'Alberta[136], de la Colombie-Britannique[137], de la Saskatchewan[138] et de l'Ontario[139].

En se basant sur le sondage effectué par la CAI auprès d'une cinquantaine d'organismes (ministères et organismes publics, villes, écoles, etc.), il est possible d'estimer à 5 000 le nombre de caméras utilisées en 2003[140]. Comme ces données excluent l'utilisation de caméras de surveillance par le secteur privé, la vidéosurveillance peut par conséquent être considérée comme un phénomène important au Québec, mais tout de même pas autant que dans d'autres pays, comme le Royaume-Uni, les États-Unis ou la France, par exemple.

Quelques définitions utiles

Une distinction primordiale s'impose d'entrée de jeu. Il existe différents types de surveillance par caméra et différents types de caméras de surveillance. Dans le premier cas, il est davantage question de la manière dont sont utilisées les caméras. Dans le second, c'est davantage les fonctionnalités des caméras qui constituent le point d'intérêt. À titre d'exemple, il serait possible de mettre en place une surveillance clandestine (type de *surveillance* par caméra) en utilisant des caméras de secteur (types de *caméras* de surveillance).

La typologie de la surveillance par caméra établie par l'Association sur l'accès et la protection de l'information (AAPI)[141] s'avère utile dans le cadre de la présente analyse. En effet, en distinguant le fonctionnement de chaque type de surveillance par caméra, il est plus facile de définir les enjeux éthiques qui leur sont propres.

Il faut noter que les types de surveillance par caméra suivants peuvent aussi être combinés. La surveillance par caméra peut donc être :

- en temps réel, les caméras étant reliées à une centrale où les images sont transmises sur des écrans en circuit fermé. Les opérateurs interviennent lorsque la situation le requiert ;
- de nature passive par un enregistrement et une lecture effectués à certains intervalles ;
- de nature active par un visionnement continu du personnel de sécurité ;
- avec enregistrement continu pour une surveillance ciblée ou générale ;
- clandestine, lorsqu'elle se fait à l'insu des individus ;
- ouverte, lorsque les caméras sont installées au vu et au su du public et que celui-ci est explicitement informé de leur présence.

En outre, il existe différents types de caméras de surveillance. La Commission s'inspire largement du mémoire présenté par l'Association canadienne de la sécurité (CANASA)[142] dans le cadre de la consultation de la CAI et du *Bilan* de cette dernière[143] pour les présenter.

Tout d'abord, il convient de distinguer les caméras de secteur, de gestion, d'identification, cachées et avec zoom.

Les caméras de secteur ou de vérification sont utilisées pour un lieu en particulier. Les caractéristiques de ce type d'appareils rendent peu probable l'identification d'une personne, la caméra filmant plus un lieu qu'un individu. Il s'agit du type de caméras le plus répandu et le plus utilisé pour l'observation d'une foule.

Quant aux caméras de gestion, elles sont utilisées la plupart du temps pour la surveillance du réseau routier parce qu'elles offrent une vue panoramique.

136. FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY, *Guide to Using Surveillance Cameras in Public Areas*, Gouvernement de l'Alberta, juin 2004. [http://foip.gov.ab.ca/resources/publications/pdf/SurveillanceGuide.pdf].

137. OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA, *Public Surveillance System Privacy Guidelines*, 26 janvier 2001. [http://www.oipcbc.org/advice/VID-SURV(2006).pdf].

138. OFFICE OF THE SASKATCHEWAN INFORMATION AND PRIVACY COMMISSIONER, *Guidelines for Video Surveillance by Saskatchewan Public Bodies*, 24 juin 2004. [www.oipc.sk.ca/webdocs/VideoSurveillance.pdf].

139. Ann CAVOUKIAN, *Guidelines for Using Video Surveillance Cameras in Public Spaces*, Information and Privacy Commissioner/Ontario, octobre 2001. [www.ipc.on.ca/images/Resources/video-e.pdf].

140. Michel LAPORTE, *op. cit.*, p. 17 et 18.

141. ASSOCIATION SUR L'ACCÈS ET LA PROTECTION DE L'INFORMATION, *L'utilisation de caméras de surveillance par des organismes publics dans des lieux publics*, Mémoire soumis à la Commission d'accès à l'information dans le cadre de la consultation publique, septembre 2003.

142. ASSOCIATION CANADIENNE DE L'ALARME ET DE LA SÉCURITÉ, *Pour un monde en toute sécurité*, Mémoire présenté à la Commission d'accès à l'information, 2 septembre 2003.

143. Michel LAPORTE, *op. cit.*, p. 54.

Les caméras d'identification sont celles qui se trouvent le plus souvent aux abords des guichets automatiques des banques et des caisses. L'objectif premier de ces caméras est l'identification des personnes transitant par un lieu précis.

Les caméras cachées assurent une surveillance secrète de certains endroits. Elles peuvent également capter un événement particulier dans le cadre de la filature d'une personne ou d'une enquête policière. Il s'agit de caméras fixes pouvant être aussi petites que la pointe d'un crayon.

Les caméras avec zoom et routine de position permettent de programmer les angles de vue et d'éviter de capter, par exemple, une rue publique ou une maison privée. Elles peuvent être utilisées, par exemple, pour assurer la surveillance d'une cour de triage.

Les secteurs d'utilisation de la vidéosurveillance

Il est facile de se perdre lorsque vient le temps d'esquisser une typologie des secteurs d'utilisation de la vidéosurveillance et des finalités de cette dernière. De fait, les secteurs sont nombreux et les fins très diversifiées. Cependant, la Commission, s'appuyant sur les travaux de la CAI, constate que, parmi les principaux secteurs d'utilisation, la sécurité publique s'avère sans doute le plus important. De plus, la prévention du crime et la lutte au sentiment d'insécurité sont les motifs les plus fréquemment évoqués[144].

Parmi les autres secteurs d'utilisation de la vidéosurveillance, il faut également souligner la gestion de la circulation automobile sur les axes routiers afin « de détecter rapidement un incident ou un problème de congestion pour en diminuer les effets, réduire le nombre d'accidents secondaires et le temps de parcours d'un usager de la route, informer en temps réel l'automobiliste et collaborer étroitement avec les services d'urgence[145] ». La demande en équipement de vidéosurveillance vient également des citoyens, pour leur usage personnel. Ceux-ci auraient recours aux caméras de surveillance pour différents motifs : filmer la chambre de leurs parents en établissement afin de s'assurer qu'ils sont bien traités, épier la gardienne pendant que les parents sont absents, etc. Des firmes privées utilisent également la vidéosurveillance, cette fois dans le but de réduire les pertes liées au vol et au vandalisme, par exemple.

Les différentes technologies actuelles et en développement et leur mode de fonctionnement

Ainsi qu'il a été mentionné précédemment, les avancées technologiques récentes ont élargi l'éventail des possibilités qu'offre la vidéosurveillance. Tout d'abord, la numérisation des images captées a entraîné une révolution dans ce domaine : la collecte, le stockage et la manipulation des données sont des opérations qui prennent alors une envergure sans précédent, notamment en raison du rôle facilitateur que jouent les technologies de l'information et des communications. D'autres innovations témoignent du fait que la vidéosurveillance est à la fine pointe de la technologie : « miniaturisation des caméras, caméras qui pivotent à 360°, dites biométriques qui enregistrent les caractéristiques faciales, à haute-résolution, à vision nocturne, dites électromagnétiques qui voient à travers les matières, à infrarouges qui détectent des variations de température, à faibles doses de rayons X qui donnent une image du corps et de tout ce qu'il transporte[146] ».

Parmi les technologies actuelles et en développement qui ont particulièrement retenu l'attention de la Commission, la reconnaissance faciale et les logiciels intelligents soulèvent des enjeux éthiques, notamment quant au respect de la vie privée, des risques de discrimination et de stigmatisation et au respect de la démocratie.

La reconnaissance faciale permet de comparer le visage d'une personne capté par la caméra de surveillance avec des photos de visages de personnes recherchées ou de présumés terroristes, par exemple.

Les logiciels intelligents, pour leur part, renferment des algorithmes permettant de repérer des comportements jugés inacceptables ou déviants chez les personnes surveillées. Par exemple, un logiciel intelligent pourrait

144. *Ibid.*, p. 15.

145. *Ibid.*, p. 16.

146. FÉDÉRATION DES TRAVAILLEURS ET TRAVAILLEUSES DU QUÉBEC, *Mémoire de la Fédération des travailleurs et travailleuses du Québec présenté à la Commission d'accès à l'information du Québec sur l'utilisation de caméras de surveillance par des organismes publics dans les lieux publics*, Montréal, 22 septembre 2003, p. 7. [http://www.ftq.qc.ca/modules/documents/index.php?id=58&langue=fr].

repérer une personne allant à contre-courant dans un mouvement de foule, puisqu'il s'agit d'un comportement qui s'écarte de la norme. Le choix des comportements devant faire l'objet d'une attention spéciale est laissé à la discrétion de l'utilisateur des caméras de surveillance. Aussi, un service de police pourrait personnaliser un logiciel intelligent pour qu'il repère des comportements associés à la vente de stupéfiants, alors qu'un service de sécurité dans une gare de métro pourrait cibler des personnes qui demeurent sur le quai après le départ d'un train.

Ces nouvelles techniques mettent en lumière le fait que la machine tend de plus en plus à se substituer à la présence d'un surveillant dans le travail d'analyse des données recueillies par les caméras de surveillance. Dans le préambule à ses lignes directrices concernant le recours à la vidéosurveillance, le Commissariat à la protection de la vie privée du Canada explique comment ces nouvelles techniques changent la donne sur le plan éthique :

> *À l'époque où l'on dépendait encore des enregistrements sur bande magnétique et qu'il fallait que quelqu'un visionne chaque geste et événement pour émettre un jugement sur une personne, l'énorme charge de travail qu'exigeait ce type de surveillance en limitait le recours. Aujourd'hui, il existe des systèmes de reconnaissance faciale et des logiciels de reconnaissance des formes permettant l'analyse d'un grand nombre d'images. Ainsi, les données recueillies font l'objet de beaucoup plus de manipulations, mais pas nécessairement par des êtres humains. Il est donc plus probable que les images enregistrées soient conservées et qu'elles fassent l'objet d'exploration de données, car les nouvelles technologies réduisent de beaucoup la somme de travail à effectuer. Cette façon de faire pose toutefois certains risques, comme les observations systématisées de groupes ou de personnes*[147].

Intégrer l'éthique dans les processus de programmation des NTSC constitue donc un défi de taille, surtout lorsque c'est une machine et non un être humain qui prend les décisions. D'ailleurs, cet enjeu éthique sera traité un peu plus loin.

Les atouts de la vidéosurveillance

La révolution numérique confère à la vidéosurveillance des atouts importants, notamment sur le plan de l'efficacité et de la diminution des coûts en matière de surveillance. Par exemple, le stockage des données (une grande quantité d'heures de visionnement peut être stockée sur un simple disque compact) et le réseautage des caméras (des réseaux de caméras de surveillance peuvent être interconnectés et un surveillant peut avoir accès à ces réseaux à distance par Internet) entraînent des économies d'échelle substantielles pour les utilisateurs. Ces économies sont en partie attribuables au fait que des machines prennent le relais des êtres humains en matière de surveillance : plutôt que de rémunérer policiers et agents de sécurité sur le terrain, certains organismes préfèrent se tourner vers l'achat d'équipement de vidéosurveillance.

Mais, pour les promoteurs de la vidéosurveillance, son principal atout réside dans sa prétendue capacité de réduire la criminalité par un effet de dissuasion. Cet effet est de plus en plus recherché dans le domaine de la lutte au terrorisme :

> *Au Canada et ailleurs dans le monde, le recours à la surveillance vidéo visant à détecter et à prévenir les activités criminelles ainsi qu'à faciliter la tenue de poursuites judiciaires a pris une ampleur considérable au cours des dernières années. Les forces policières et les autorités chargées de l'application de la loi considèrent de plus en plus qu'il s'agit d'un moyen légitime de mettre un frein à la criminalité, y compris le terrorisme. Dans le contexte mondial actuel, les pouvoirs publics s'intéressent de plus en plus à la mise en place de systèmes de surveillance vidéo dans les lieux publics. Au Royaume-Uni, la surveillance vidéo est devenue pratique courante. Aux États-Unis et au Canada, les pouvoirs publics et les responsables de la lutte antiterroriste y ont de plus en plus recours, surtout depuis les événements de septembre 2001*[148].

Toutefois, des nuances essentielles qui révèlent certaines failles de la vidéosurveillance sont apportées par différents acteurs dans le domaine.

Les failles de la vidéosurveillance

Ce n'est pas tant la fiabilité de l'équipement que l'efficacité de la vidéosurveillance en matière de dissuasion qui est pointée du doigt comme étant une faille de cette technologie. Selon une méta-analyse britannique sur le sujet, la vidéosurveillance aurait un effet, quoique

147. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *op. cit.*
148. *Ibid.*

minime, amenant une diminution du crime[149]. Des nuances importantes méritent cependant d'être apportées. Si une majorité d'études tendent à montrer un effet dissuasif, d'autres, moins nombreuses, montrent un effet contraire[150]. Qui plus est, l'efficacité de la vidéosurveillance diffère selon le type de crime commis. Si cette technologie s'avère efficace contre le vol de voiture, elle ne l'est nullement pour contrer les crimes violents[151].

L'impact géographique et urbain de l'implantation massive de ce type de technologie sur la délinquance est encore matière à débat. Dans l'attente de résultats scientifiques probants, la Commission s'interroge elle aussi sur les risques de déplacement de la criminalité : la surveillance d'un endroit bien précis pour y faire chuter la criminalité encouragerait les criminels à migrer vers des endroits moins surveillés.

Enfin, si la vidéosurveillance peut avoir un effet dissuasif chez certains criminels, force est de reconnaître que d'éventuels terroristes prêts à mourir afin de perpétrer un attentat ne se soucient guère d'être filmés et ainsi reconnus. Tout au plus les caméras de surveillance peuvent-elles filmer les terroristes avant que ceux-ci ne passent aux actes (ce qui pourrait peut-être aider à déjouer des complots d'attentats) ou encore pendant et après un attentat, ce qui peut guider les autorités afin de les identifier et, le cas échéant de les retrouver s'ils sont toujours vivants.

Le marché de la vidéosurveillance

L'avenir du marché de la vidéosurveillance s'annonce pour être sous le signe de l'expansion, notamment en raison des inquiétudes à l'égard d'éventuels actes terroristes, mais également parce que plusieurs organisations remplaceront probablement leur équipement pour passer à la technologie IP[152]. De 2006 à 2009, le marché mondial de la vidéosurveillance devrait par conséquent croître de 37 %[153].

L'intérêt de la population

D'une manière générale, la population voit d'un bon œil l'installation de caméras de surveillance à des fins de sécurité. En effet, il est rassurant de savoir que des lieux publics sont surveillés et qu'en cas d'incident quelqu'un peut nous venir en aide. De plus, comme la plupart des gens affirment ne rien avoir à se reprocher, la vidéosurveillance les laisse relativement indifférents. Un sondage mené par *La Toile de Sherbrooke* en mai 2004 montre que, lorsque la question de l'utilisation de la vidéosurveillance à des fins de sécurité est posée, les répondants estiment être en accord avec cette méthode dans une proportion de 82 %. Dans un sondage plus récent, les répondants devaient choisir le niveau de soutien qu'ils témoignaient à l'égard de diverses mesures antiterroristes. L'installation de caméras de surveillance dans tous les endroits publics récoltait 72 % d'appui. Pour le Québec seulement, la proportion de ceux qui appuient une telle mesure grimpe à 77 %.

En Europe, une majorité de répondants à une vaste enquête dans cinq pays se disent en faveur de la vidéosurveillance dans leur ville[154]. Toutefois, le degré d'acceptation diffère grandement selon le contexte dans lequel seraient utilisées les caméras : très bien acceptée pour des environnements comme les institutions financières et les transports en commun, la vidéosurveillance n'est pas la bienvenue dans des endroits plus privés, comme les vestiaires[155].

L'identification par radiofréquence (IRF) : vers l'intelligence ambiante ?

La technologie d'identification par radiofréquence (IRF)[156] trouve des applications aussi nombreuses que diversifiées. La décrire en quelques mots relève donc de l'impossible. De plus, la nature même de la technologie, soit celle d'un émulateur de fonctionnalités, ne se

149. Brandon C. WELSH et David P. FARRINGTON, *Crime Prevention Effects of Closed Circuit Television : a Systematic Review*, Home Office Research Study 252, août 2002, p. 41. [http://www.homeoffice.gov.uk/rds/pdfs2/hors252.pdf].

150. *Ibid.*

151. *Ibid.*, p. 42.

152. « Research : World CCTV Market to Grow 37 Percent by 2009 », *SecurityInfoWatch.com* [en ligne], 14 juillet 2006. [http://www.securityinfowatch.com/online/Research--Studies-and-Whitepapers/87028IW321].

153. *Ibid.*

154. Leon HEMPEL et Eric TOPFER, *CCTV in Europe, Final Report*, Working Paper No. 15, août 2004, p. 42. [http://www.urbaneye.net/results/ue_wp15.pdf].

155. *Ibid.*

156. Dans le cadre du présent avis, la Commission a retenu l'expression francisée de *Radio Frequency Identification* ou *RFID*.

limitant pas à une application bien spécifique[157], elle rend son analyse un peu plus complexe. Aussi, une précision préliminaire s'impose : comme le présent avis s'intéresse à des technologies à des fins de sécurité, il y sera surtout question des applications en ce domaine. Des finalités dans d'autres secteurs pourront cependant être mentionnées au passage. Mais, avant tout, il semble indispensable de donner quelques définitions qui permettront de mieux comprendre les finalités associées à l'IRF et le mode de fonctionnement de celle-ci.

Quelques définitions utiles

Deux composantes principales rendent l'IRF possible. Tout d'abord, **une puce** dotée « d'un circuit électronique qui stocke des données et une antenne qui communique les données au moyen d'ondes radio[158] ». Cette puce communique avec **un lecteur**. Celui-ci possède « une antenne et un démodulateur qui traduit l'information analogique [...] en données numériques. L'information numérique peut alors être traitée par un ordinateur[159]. »

Les finalités associées à l'IRF

Les finalités associées à l'IRF sont si nombreuses que seulement les plus communes seront mentionnées. En matière de sécurité, l'IRF est utilisée depuis peu dans les documents d'identité tels que les passeports. Les puces d'IRF contenues dans les passeports américains[160] et de plusieurs pays de l'Union européenne[161] contiennent des données biométriques qui peuvent être lues par des lecteurs aux postes frontaliers. La fonction principale d'une telle application est de combattre la fraude dans le domaine des documents d'identité et le vol d'identité. Autre fonction, le contrôle de l'accès des personnes à des zones réglementées (dans les aéroports, par exemple) peut aussi être gérée par des systèmes d'IRF[162]. Les personnes autorisées, une fois munies de cartes dotées d'une puce d'IRF, peuvent déverrouiller les accès à ces zones.

Les différentes technologies actuelles et en développement et leur mode de fonctionnement

L'IRF repose sur l'utilisation d'une puce électronique munie d'une antenne miniature susceptible d'être activée par un lecteur spécifique et de lui transmettre des informations. Cette technologie peut être passive, c'est-à-dire que la puce est dépourvue de réserve d'énergie. Elle est activée par des fréquences radio envoyées par un lecteur d'IRF et elle utilise l'énergie du signal radio reçu pour le refléter et y répondre. Cette façon d'opérer demeure la plus répandue. La puce d'IRF active possède une batterie interne et dispose d'un plus grand rayonnement en fonction du lecteur utilisé[163].

Une grande variété de formes et de tailles caractérise les puces d'IRF[164]. Certaines sont peu subtiles, comme les étiquettes antivol attachées aux vêtements dans certaines boutiques. D'autres peuvent être aussi petites qu'un grain de riz et peuvent ainsi être implantées sous la peau. C'est le cas des puces implantées chez certains animaux de compagnie ou chez des espèces en danger. Enfin, les travaux se poursuivent pour être en mesure de développer des puces si petites qu'elles pourraient être intégrées à la monnaie de papier afin d'éviter la contrefaçon.

157. COMMISSION EUROPÉENNE, *Your Voice on RFID. Background Document for Public Consultation on Radio Frequency Identification (RFID) – Summary of Five Workshops*, juillet 2006, p. 6. [http://www.rfidconsultation.eu/docs/ficheiros/Your_voice_on_RFID.pdf].

158. GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL DU PARLEMENT EUROPÉEN ET DU CONSEIL, *Document de travail sur les questions de protection des données liées à la technologie RFID (radio-identification)*, Bruxelles, 19 janvier 2005, p. 3 et 4. [http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_fr.pdf].

159. *Ibid.*

160. DEPARTMENT OF STATE, « Department of State Begins Issuing Electronic Passports to the Public », Communiqué de presse, 14 août 2006.

161. Guillaume DELEURENCE, « Le passeport se convertit à l'électronique, avant la biométrie », *01net.com* [en ligne], 28 août 2006. [http://www.01net.com/editorial/324183/societe/le-passeport-se-convertit-a-l-electronique-avant-la-biometrie/].

162. GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL DU PARLEMENT EUROPÉEN ET DU CONSEIL, *op. cit.*, p. 5.

163. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *La technologie d'identification par radiofréquence (RFID) : doit-on s'en méfier ?*, Document d'analyse, mai 2006, p. 1. [http://www.cai.gouv.qc.ca/06_documentation/01_pdf/Analyse_RFID.pdf].

164. ELECTRONIC PRIVACY INFORMATION CENTER, « Radio Frequency Identification (RFID) Systems », *epic.org* [en ligne], 13 janvier 2006. [http://www.epic.org/privacy/rfid/].

Le transfert des données entre la puce d'IRF passive et un lecteur peut se faire en quatre types de fréquences[165] :

- Basse fréquence (100-500 kHz). Son rayon d'action est de moins d'un mètre. Cette technologie demande une antenne de grande dimension dont le coût est relativement élevé et elle est principalement utilisée dans le domaine du contrôle de l'accès à des lieux et pour l'étiquetage des animaux.
- Haute fréquence (10-15 MHz). Son rayon d'action est d'approximativement un mètre. Cette technologie est la plus répandue et elle est utilisée dans le contrôle de l'accès à certains lieux, pour l'étiquetage d'articles chez certains détaillants, dans les bibliothèques et dans les transports.
- Ultra haute fréquence (850-1 000 MHz) – Son rayon d'action varie de quatre à cinq mètres. Cette technologie, appelée à remplacer la haute fréquence, est utilisée notamment dans la gestion des inventaires.
- Micro-ondes (2,4-5,8 GHz) – Son rayon d'action est d'environ un mètre. Cette technologie est hautement sujette aux interférences, ce qui confine son utilisation à des cartes de paiement rapide (*speed passes*).

Le fonctionnement et les applications de l'IRF ont un impact direct sur leur possible encadrement normatif. Étant donné que la technologie en est encore au stade du développement, certains suggèrent un encadrement qui prendrait la forme d'une autorégulation par l'industrie. Des lignes directrices pourraient ainsi venir compléter les lois déjà existantes et qui balisent la gestion des renseignements personnels[166]. Évidemment, un tel schéma d'encadrement restreint considérablement la possibilité de sanctionner les délinquants. C'est d'ailleurs pourquoi certains proposent la mise en place d'un ombudsman spécialement affecté aux plaintes issues de consommateurs de produits contenant des puces d'IRF[167].

L'IRF est une technologie bien particulière en matière de renseignements personnels. Si l'introduction d'une puce contenant des données biométriques dans un passeport constitue clairement un exemple d'application de la législation sur la gestion des renseignements personnels, il pourrait en aller autrement d'autres applications.

À ce propos, le Groupe de travail sur la protection des personnes à l'égard du traitement des données à caractère personnel du Parlement européen et du Conseil (appelé Groupe de l'article 29 ci-après) émet la réflexion suivante :

> *On peut alors se demander si cela signifie que la directive Protection des données s'applique nécessairement à la collecte de données par la technologie RFID. La réponse dépendra en général de l'application concrète spécifique de la technologie de radio-identification, et plus particulièrement du point de savoir si l'application RFID spécifique comporte le traitement de données à caractère personnel telles qu'elles sont définies par la directive générale Protection des données*[168].

Les atouts de l'IRF

Comme c'est le cas avec plusieurs technologies émergentes, les applications de l'identification par radiofréquence font naître de nombreuses promesses. Parmi celles-ci, l'IRF pourrait contribuer à l'amélioration de la logistique dans la chaîne de distribution des produits de consommation, favoriser une traçabilité plus fine des produits, une meilleure prévention du vol et une détection plus efficace de la contrefaçon[169]. Les puces d'IRF, contrairement aux code-barres actuels, peuvent être lues à distance, et ce, à travers la neige, le brouillard, la glace ou encore la peinture, ce qui rend leur utilisation plus fiable et d'autant plus intéressante[170].

Dans un futur rapproché, l'IRF permettrait de suivre les personnes à la trace dans l'espace et le temps. Le fait de pouvoir garder une personne sous surveillance par un tel

165. Teresa SCASSA *et al.*, *An Analysis of Legal and Technological Privacy Implications of Radio Frequency Identification Technologies*, préparé pour le Commissariat à la protection de la vie privée du Canada, 28 avril 2005, p. 6.

166. COMMISSION EUROPÉENNE, *Your Voice on RFID, Background Document for Public Consultation on Radio Frequency Identification (RFID)* – Summary of Five Workshops, juillet 2006, p. 14. [http://www.rfidconsultation.eu/docs/ficheiros/Your_voice_on_RFID.pdf].

167. *Ibid.*

168. GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL DU PARLEMENT EUROPÉEN ET DU CONSEIL, *op. cit.*, p. 9.

169. COMMISSION EUROPÉENNE, *RFID Security, Data Protection and Privacy, Health and Safety Issues*, Policy Framework Paper [en ligne], 11 mai 2006. [http://www.rfidconsultation.eu/41/38/264.html].

170. ELECTRONIC PRIVACY INFORMATION CENTER, *op. cit.*

moyen peut constituer un atout de cette technologie pour les autorités policières, par exemple. L'implantation de puces d'IRF dans le corps humain comporte également son lot de bénéfices attendus : une telle puce (à la fois minuscule et durable) peut contenir de l'information sur l'identité, les caractéristiques physiologiques, sur la santé et sur la nationalité de son porteur[171].

Les failles de l'IRF

Le passeport électronique muni d'une puce d'IRF contenant des informations biométriques venait tout juste d'être mis en circulation que, déjà, certains experts en sécurité des documents électroniques ont relevé des failles importantes dans les puces d'IRF qui permettent de dupliquer l'information disponible sur la puce et de produire d'autres passeports identiques[172]. Cette démonstration ainsi que la perspective de voir les puces d'IRF introduites dans d'autres documents d'identité ont ravivé les craintes déjà exprimées par plusieurs organismes quant aux risques de fraude dans ce type de documents. L'absence de procédés de chiffrement dans les puces d'IRF sème d'autant plus le doute sur leur capacité à protéger les renseignements qu'elles contiennent.

Au Québec, la CAI a aussi soulevé un questionnement quant aux retombées de l'introduction de puces d'IRF dans les documents d'identité : « Il y a lieu de se demander si l'incorporation de puces RFID contenant des renseignements personnels dans le permis de conduire ou dans le passeport n'aura pas comme effet d'augmenter les risques d'usurpation d'identité[173]. »

Une autre faille d'importance est étroitement liée à un des atouts de l'IRF. La lecture à distance ouvre en effet la porte au repérage clandestin : une personne non autorisée pourrait lire à distance le contenu de la puce, et ce, à l'insu du porteur de la puce[174]. En matière de sécurité, et dans le contexte actuel où les terroristes cherchent à cibler leurs attaques, le repérage clandestin pourrait servir à des terroristes désireux de « trier » leurs victimes éventuelles dans une foule selon leur nationalité, par exemple[175].

La duperie apparaît comme un autre moyen de tromper les systèmes d'IRF[176] : une personne mal intentionnée peut transmettre de fausses informations soit vers le lecteur, soit vers la puce d'IRF ou encore perpétrer une attaque du type *Denial of Service* (DoS) – la disponibilité du système d'IRF peut alors être compromise.

Il demeure donc très important de signaler que la lecture par radiofréquence n'est pas précise à 100 % et que les systèmes qui la soutiennent, comme les bases de données, sont aussi sujets que d'autres aux attaques. Selon la Commission européenne, la recherche et le développement sont encore nécessaires dans le cas de certaines applications[177]. En somme, la technologie IRF, prise globalement, se trouve encore au stade du développement.

Le marché de l'IRF

Bien que la technologie d'identification par radiofréquence existe depuis la Deuxième Guerre mondiale, ce n'est que récemment, et grâce à l'amélioration notable de la technologie, que le marché a pris une ampleur considérable. Durant les soixante années qui séparent 1946 de 2006, c'est 2,5 milliards de puces d'IRF qui ont été vendues, y compris les 600 millions vendues en 2005 seulement[178]. Les prévisions pour l'année 2006 étaient de 1,3 milliard de puces vendues[179]. Sur le total des puces vendues, la

171. Kenneth R. FOSTER et Jan JAEGER, « RFID Inside. The Murky Ethics of Implanted Chips », dans *IEEE Spectrum*, mars 2007, p. 27. [http://pages.cs.wisc.edu/~markhill/cs252/Spring2007/handouts/spectrum07_rfid_ethics.pdf].

172. Kim ZETTER, « Hackers Clone E-Passports », *Wired.com*. [en ligne]. 3 août 2006. [http://www.wired.com/science/discoveries/news/2006/08/71521].

173. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *La technologie d'identification par radiofréquence (RFID) : doit-on s'en méfier ?*, Document d'analyse, mai 2006, p. 3 et 4. [http://www.cai.gouv.qc.ca/06_documentation/01_pdf/Analyse_RFID.pdf].

174. GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL DU PARLEMENT EUROPÉEN ET DU CONSEIL, *op. cit.*, p. 8.

175. *Ibid.*

176. COMMISSION EUROPÉENNE, *RFID Security, Data Protection and Privacy, Health and Safety Issues*, Policy Framework Paper [en ligne], 11 mai 2006, p. 9. [http://www.rfidconsultation.eu/41/38/264.html].

177. COMMISSION EUROPÉENNE, *Your Voice on RFID. Background Document for Public Consultation on Radio Frequency Identification (RFID) – Summary of Five Workshops*, juillet 2006, p. 15. [http://www.rfidconsultation.eu/docs/ficheiros/Your_voice_on_RFID.pdf].

178. IDTECHEX, *RFID Forecast, Players & Opportunities 2006-2016*, octobre 2006.

179. *Ibid.*

part des puces de type passif représente les trois quarts du marché, les puces de type actif complétant avec le quart qui reste[180].

Si l'industrie est en mesure de relever les nombreux défis qui caractérisent cette technologie émergente, tels que le coût de fabrication encore trop élevé ainsi que le manque de fiabilité et d'harmonisation sur le plan de la fréquence utilisée, une croissance exponentielle est prévue pour le marché de l'IRF : d'un marché estimé à 2,7 milliards de dollars américains en 2006, l'IRF deviendrait un marché de 26,2 milliards en 2016[181].

En 2004, c'est le secteur de la sécurité qui accaparait la plus grande part du marché de l'IRF[182]. Depuis, la part de marché des puces destinées à la gestion des inventaires a largement augmenté. Les observateurs prévoient une baisse du coût de fabrication des puces d'IRF. Une fois cette étape franchie, la part de marché de l'étiquetage individuel des médicaments, des animaux, des bagages, des livres, etc., sera également appelée à augmenter[183].

L'intérêt de la population

De récentes études menées aux États-Unis et en Europe montrent que la population en général n'a pas encore une opinion bien arrêtée sur la technologie d'identification par radiofréquence et qu'elle demande à en savoir plus[184]. La Commission européenne arrive à la même conclusion et, considérant que les consommateurs ne sont pas suffisamment sensibilisés à la potentielle invasion de leur vie privée par les nouvelles technologies telles que l'IRF, elle recommande la tenue d'une campagne d'information en la matière[185].

Les personnes interrogées, en tant que consommateurs, escomptent de l'IRF des bénéfices et ils appréhendent également certaines retombées négatives. D'une part, elles s'attendent notamment à ce que l'IRF permette de retrouver des objets volés plus rapidement, qu'elle s'intègre à des dispositifs antivol pour les voitures, qu'elle améliore la sécurité alimentaire, qu'elle entraîne une réduction des coûts de production et, par conséquent, une réduction du prix d'achat des produits[186].

D'autre part, les consommateurs américains et européens craignent que l'IRF ne facilite l'utilisation de données les concernant par des tiers, une recrudescence des campagnes de marketing et la possibilité de suivre les consommateurs à la trace par les achats qu'ils font[187]. Les enjeux environnementaux et en santé constituent des enjeux secondaires dans l'esprit des répondants.

* * *

Le fait d'aborder chacune des NTSC tour à tour impose à la Commission une limite importante dans son analyse : elle est en effet contrainte de négliger la convergence des différentes NTSC dans des systèmes de sécurité. Or, certains exemples sont déjà mis en application, comme l'utilisation de logiciels de reconnaissance faciale (biométrie) avec des images captées par des caméras de surveillance (vidéosurveillance) ou encore l'introduction de données biométriques sur des puces d'IRF dans les passeports. Selon les experts consultés, la convergence des NTSC n'entraîne pas seulement une addition des risques qui leur sont associés, mais plutôt une multiplication de ceux-ci.

180. COMMISSION EUROPÉENNE, *RFID Security, Data Protection and Privacy, Health and Safety Issues*, Policy Framework Paper [en ligne], 11 mai 2006. [http://www.rfidconsultation.eu/41/38/264.html].

181. IDTECHEX, *op. cit.*

182. COMMISSION EUROPÉENNE, *RFID Security, Data Protection and Privacy, Health and Safety Issues*, Policy Framework Paper [en ligne], 11 mai 2006. [http://www.rfidconsultation.eu/41/38/264.html].

183. *Ibid.*

184. CAP GEMINI ERNST & YOUNG, *RFID and Consumers, Understanding Their Mindset, A U.S. Study Examining Consumer Awareness and Perceptions of Radio Frequency Identification Technology*, Executive Summary, 13 janvier 2004, p. 2. [http://www.rfidconsultation.eu/docs/ficheiros/CPRD_RFID_mindset_ES.pdf] et Helen DUCE, Executive Briefing, Public Policy : Understanding Public Opinion, Auto-ID Centre, 1er février 2003. [http://www.autoidlabs.org/single-view/dir/article/6/199/page.html].

185. COMMISSION EUROPÉENNE, *Your Voice on RFID, Background Document for Public Consultation on Radio Frequency Identification (RFID) – Summary of Five Workshops*, juillet 2006, p. 15. [http://www.rfidconsultation.eu/docs/ficheiros/Your_voice_on_RFID.pdf].

186. CAP GEMINI ERNST & YOUNG, *op. cit.*, p. 2.

187. *Ibid.*

Chapitre 3
Un regard éthique sur les nouvelles technologies de surveillance et de contrôle : à la recherche d'un juste équilibre entre les valeurs

Le déploiement des nouvelles technologies de surveillance et de contrôle (NTSC) révèle en bonne partie l'importance accordée aux valeurs fondamentales au sein des sociétés démocratiques. Dans un contexte de sociétés en proie à un sentiment d'insécurité régulièrement ravivé par les médias et où le risque et la surveillance occupent une place prépondérante, un regard éthique sur le déploiement des NTSC s'avère essentiel. Ainsi, l'évaluation de la pertinence, de l'efficacité et de la fiabilité des NTSC, la proportionnalité de la réponse à l'insécurité, l'acceptabilité sociale, le consentement, le respect des finalités et la protection des renseignements personnels constituent les principaux points d'intérêt retenus par la Commission.

À la suite des événements du 11 septembre 2001, bon nombre des mesures de sécurité mises en place ont eu pour effet de renforcer le pouvoir des gouvernements et des systèmes judiciaire et policier, notamment pour leur permettre d'exiger des citoyens des renseignements personnels beaucoup plus détaillés qu'auparavant et d'y accéder à d'autres fins que celles pour lesquelles elles ont été initialement fournies[188]. En marge de ce phénomène, s'observent également les pratiques des acteurs privés qui sont également friands de systèmes de sécurité de plus en plus performants. Cette tendance illustre assez bien à quel point la valeur de sécurité prend une importance grandissante, peut-être au détriment d'autres valeurs fondamentales au sein des sociétés démocratiques, par exemple les libertés individuelles. À l'intérieur de plusieurs problématiques en matière de sécurité, les valeurs de sécurité et de liberté entrent souvent en conflit. Toutefois, rien ne prouve que certains compromis soient hors d'atteinte.

Qui plus est, la prudence s'impose à l'endroit des discours s'articulant autour de l'idée selon laquelle il faut repenser l'équilibre entre le pouvoir de l'État et les libertés individuelles. Ces concepts ne sont pas quantifiables et ne peuvent par conséquent faire l'objet d'un équilibre « mathématique ». En outre, si la perte de libertés est tangible, les gains qui devraient en découler en matière de sécurité sont, pour leur part, beaucoup plus difficiles à appréhender et à garantir.

Ces considérations appellent un examen minutieux de la justification morale de l'abandon des droits et libertés individuels, d'autant plus qu'habituellement l'abandon de certains droits individuels dans le cadre d'une conjoncture particulière et passagère demeure risqué – ces droits étant difficiles à reprendre par la suite. Ainsi, la Commission invite à la vigilance et souligne les risques associés aux discours qui prônent l'abandon de droits et libertés au profit d'une plus grande sécurité.

L'image de l'équilibre ne doit donc pas être considérée pour autre chose que ce qu'elle est : une représentation d'un phénomène éminemment complexe. De fait, aucune image ne pourrait rendre parfaitement les interrelations étroites entre la liberté et la sécurité. Ces deux valeurs sont en fait deux conditions fondamentales de la vie démocratique. Et chacune peut potentiellement brimer et favoriser l'autre. Dans le cadre du présent avis, ce phénomène peut s'illustrer de la façon suivante : l'émergence des NTSC est intimement liée à la volonté de l'État et d'autres organisations d'assurer une plus grande sécurité sur leur territoire. Cette incarnation du pouvoir de l'État vise à préserver la démocratie, mais, paradoxalement, elle s'attaque à des droits et libertés fondamentaux représentatifs des sociétés démocratiques. Il faut reconnaître que les NTSC peuvent contribuer à assurer une meilleure sécurité. Toutefois, leur déploiement ne doit pas seulement viser l'amélioration de la sécurité, mais aussi le respect des droits et libertés des citoyens.

188. INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES, *op. cit.*, p. 4.

Entre, d'une part, l'idéal qui consisterait à promouvoir à la fois les valeurs de sécurité et de liberté et non l'une au dépend de l'autre et, d'autre part, la réalité où un choix s'avère nécessaire entre ces deux valeurs, il existe un gouffre. Si la Commission préférerait faire la promotion des deux valeurs à la fois, elle demeure bien consciente que, dans la vaste majorité des cas, une certaine forme d'arbitrage, de compromis ou d'équilibre devra être atteinte. Le défi consiste donc à atteindre un juste équilibre.

Enfin, la Commission attire l'attention sur le risque de perte d'autonomie sous-jacent au déploiement des NTSC. En effet, du simple fait qu'elle se sait surveillée une personne peut modifier son comportement. Ainsi, des citoyens, sachant qu'ils seront l'objet d'une vidéosurveillance, pourraient craindre des représailles à la suite d'une participation à des manifestations publiques ou d'une critique ouverte des décisions gouvernementales. Ce n'est par conséquent pas seulement les droits et libertés des citoyens qui sont menacés, mais bien leur autonomie, l'expression même de leur liberté. Le respect de l'autonomie des citoyens, lorsqu'il vise à leur permettre de participer pleinement à la vie démocratique, constitue la valeur fondamentale pour la préservation de l'idéal démocratique.

L'évaluation de la pertinence, de l'efficacité et de la fiabilité des NTSC : une étape préalable

Pour que les NTSC soient légitimes dans leur déploiement, non seulement leur innocuité pour la santé doit être démontrée, mais ces technologies doivent également être jugées pertinentes, efficaces et fiables. Le critère de pertinence consiste à savoir si les NTSC s'avèrent le meilleur moyen pour répondre au besoin reconnu en matière de sécurité. Ainsi, d'autres moyens moins intrusifs sur le plan de la vie privée devraient être privilégiés.

Pour que les NTSC soient efficaces, il faut que les résultats obtenus par leur déploiement correspondent aux visées d'origine.

De plus, les NTSC doivent être fiables, c'est-à-dire qu'il faut éviter que leur fonctionnement ne soulève plus de problèmes qu'elles n'apportent de solutions.

Pour être en mesure de justifier le déploiement des NTSC, il faudrait que les NTSC atteignent un niveau plus élevé de pertinence, d'efficacité et de fiabilité. D'ailleurs, au deuxième chapitre, sont présentées les principales failles de chacune des technologies abordées dans le présent avis. Mais comment déterminer la pertinence, l'efficacité et la fiabilité de ces techniques ? À qui échoit la responsabilité d'en faire la démonstration ? À ses promoteurs ? À des instances publiques ? Ces questions d'ordre technique exigent des réponses. Les mécanismes d'évaluation et leurs résultats doivent être accessibles à la population dans une forme facile à comprendre. La valeur de transparence à l'endroit de la population occupe donc une place prépondérante.

Bien que la population en général ait confiance dans la capacité de la technologie à traiter des données, il faut demeurer conscient que les programmes informatiques traitant les données recueillies par les NTSC peuvent contenir des erreurs ou encore être corrompus[189]. De plus, ce serait une erreur que de présenter les NTSC à des fins de sécurité comme étant invulnérables. Le déploiement de technologies perçues comme fiables et qui contribueraient à répandre un faux sentiment de sécurité dans la population serait inacceptable.

La Commission invite donc les acteurs concernés à entamer une réflexion quant à l'évaluation de la pertinence, de l'efficacité et de la fiabilité des NTSC. Elle estime aussi nécessaire de rappeler l'importance de déployer des technologies efficaces et fiables afin d'éviter de causer des préjudices à des personnes innocentes. Plus les NTSC seront réputées pertinentes, efficaces et fiables, plus il sera difficile pour des personnes soupçonnées de prouver leur innocence. Aussi la Commission craint-elle qu'un renversement du fardeau de la preuve ne devienne la norme et non l'exception si les NTSC permettent d'identifier des suspects.

La proportionnalité de la réponse à l'insécurité : pour un déploiement modéré

Considérant ce qui a été dit au chapitre 1 en matière de sentiment d'insécurité et compte tenu du fait que le Canada peut se considérer comme un pays généralement

189. UNESCO, *Ethical Implications of Emerging Technologies : A Survey*, Paris, UNESCO, 2007, p. 14. [unesdoc.unesco.org/images/0014/001499/149992f.pdf].

sécuritaire, la réponse à l'insécurité que constituent les NTSC ne devrait pas prendre une ampleur disproportionnée. Avec le Comité consultatif national d'éthique pour les sciences de la vie et de la santé (CCNE), la Commission estime que la « notion de proportionnalité des moyens[190] » doit être prise en considération non seulement dans le cadre des systèmes biométriques, mais dans le déploiement des NTSC en général. Mettre en place des moyens de surveillance trop intrusifs sur le plan de la vie privée compte tenu des fins visées et du contexte, tout comme « intégrer des données personnelles au-delà de ce qui est nécessaire à la finalité déclarée[191] », n'est pas justifiable. C'est entre autres pourquoi il est important de miser sur un déploiement modéré et calibré en fonction des besoins réels en matière de sécurité et non en fonction du sentiment d'insécurité que peuvent susciter des événements spectaculaires comme des attentats terroristes. Aussi, la Commission invite les décideurs politiques et privés à procéder à une évaluation et à une interprétation nuancées et lucides des besoins en matière de NTSC à des fins de sécurité.

Il est primordial que l'évaluation du rapport entre la fiabilité technique, la proportionnalité de la réponse à l'insécurité et le degré d'intrusion dans la vie privée soit faite pour chaque projet de déploiement de NTSC. Il apparaît qu'une telle évaluation serait à même de permettre un regard éthique sur les finalités pour lesquelles les NTSC sont concrètement déployées. Une telle procédure serait inédite et elle aurait pour avantage indéniable de positionner le Québec comme un meneur sur le plan de l'évaluation éthique des utilisations de ce type de technologies.

Par ailleurs, au cœur de l'évaluation de la proportionnalité de la réponse à l'insécurité se trouvent des acteurs trop souvent ignorés par les décideurs publics et privés : les fournisseurs et les installateurs de NTSC. Ceux-ci se trouvent en première ligne en ceci qu'ils doivent répondre aux besoins d'organisations publiques et privées en matière de sécurité sur le plan technique. Il est important qu'ils soient en mesure de bien conseiller leurs clients en matière de NTSC et surtout de répondre à la question suivante : Quel système de sécurité est-il recommandé d'installer en fonction du degré de sécurité qu'il faut assurer ? Les fournisseurs et les installateurs sont les premiers confrontés aux enjeux éthiques mentionnés par la Commission. Aussi est-il nécessaire qu'ils soient sensibilisés à ces questions pour que le déploiement des NTSC se fasse en accord avec les valeurs privilégiées. La question centrale semble être de savoir comment parvenir à une proportionnalité dans la réponse à l'insécurité dans un contexte de marché en croissance très rapide où la logique du profit l'emporte souvent sur la logique éthique. De telles considérations invitent à une réflexion approfondie sur la régulation des NTSC. Or, de récents développements sur le plan législatif permettraient de diffuser le fruit de cette réflexion parmi les acteurs du milieu.

Au Québec, la nouvelle Loi sur la sécurité privée encadre notamment « les activités reliées aux systèmes électroniques de sécurité, soit l'installation, la réparation, l'entretien et la surveillance continue à distance de systèmes d'alarme contre le vol ou l'intrusion, de systèmes de surveillance vidéo ou de systèmes de contrôle d'accès, à l'exception d'un système sur un véhicule routier [...][192] ». La Loi précise entre autres que le futur Bureau de la sécurité privée dispensera de la formation aux représentants des titulaires de permis d'agence et que le gouvernement pourra, par règlement, déterminer quelle est la formation nécessaire pour l'utilisation d'équipement ou décider de la formation à exiger pour la délivrance d'un permis d'agent[193]. Cette formation devrait prévoir un volet obligatoire sur les enjeux éthiques. C'est pourquoi :

> **la Commission recommande que la formation dispensée par le Bureau de la sécurité privée aux représentants des titulaires de permis d'agence inclue un volet éthique obligatoire qui s'inspirera des enjeux éthiques soulevés dans le présent avis et que le gouvernement, conformément à la Loi sur la sécurité privée, adopte la réglementation nécessaire pour que la formation exigée pour la délivrance d'un permis d'agent prévoie également un tel volet éthique.**

190. COMITÉ CONSULTATIF NATIONAL D'ÉTHIQUE POUR LES SCIENCES DE LA VIE ET DE LA SANTÉ, *Biométrie, données identitaires et droits de l'homme*, Avis n° 98, 26 avril 2007, p. 14. (www.comite-ethique.fr/docs/fr/avis098.pdf).

191. *Ibid.*

192. L.R.Q., chapitre S-3.5, 2006, c. 23, a. 1.

193. L.R.Q., chapitre S-3.5, 2006, c. 23, a. 41, 111 et 112.

L'acceptabilité sociale : une condition essentielle

Le déploiement des NTSC et le progrès quasi constant de ces technologies apparaissent souvent comme inéluctables. Une telle perception sous-tend que ces processus se déroulent sans que le débat public soit nécessairement engagé auparavant. Dans son avis sur la biométrie, le Comité consultatif national d'éthique pour les sciences de la vie et de la santé estime que « [l]a première interrogation d'ordre éthique résulte de ce caractère ressenti comme inéluctable sans que se soit instauré un débat public et sérieux sur les risques que peut comporter cette évolution et les dérives auxquelles elle expose[194] ». Cette inéluctabilité est souvent perçue comme émanant de la pression pour une plus grande efficience sur le plan économique, ce qui empêche trop souvent de prendre le recul nécessaire pour aborder la question des valeurs en jeu, mais surtout du type de société dans laquelle nous voulons vivre[195].

En considérant la popularité actuelle des gouvernements qui font de la sécurité leur cheval de bataille et à la lumière des résultats de sondages et d'enquêtes sur l'acceptation des NTSC par la population, il semble que le déploiement des NTSC ne soit pas contraire à la volonté populaire. La Commission s'interroge toutefois sur le niveau de connaissance du public en matière de biométrie, de vidéosurveillance et d'IRF. Aussi toute forme de consultation sur les NTSC doit-elle faire une place importante à la population en général et chercher d'abord et avant tout à recueillir des opinions éclairées.

Le consentement : un concept difficilement transposable dans le contexte des NTSC

La plupart du temps, il est tout simplement impossible pour les personnes surveillées de consentir à ce qu'il en soit ainsi. En fait, le consentement libre et éclairé, sur une base individuelle, n'est tout simplement pas un concept opérationnel lorsque vient le temps de l'appliquer aux NTSC. Ce qui ne veut pas dire qu'un tel état de fait ne soulève pas de questions d'ordre éthique, au contraire.

En matière de biométrie, « le consentement et la transparence [peuvent] être optionnels dans certaines mises en œuvre d'applications biométriques[196] ». Comment cela est-il possible ? Les gens laissent quotidiennement des empreintes digitales sur ce qu'ils touchent ou ils perdent des cheveux (ADN), ils échangent à voix haute (reconnaissance par la voix), se servent d'un ordinateur (rythme de la frappe au clavier), et ces éléments d'identification sont relativement faciles à recueillir. Ensuite, des données biométriques peuvent être extraites de ces éléments. La possibilité de recueillir des données biométriques à l'insu des individus (et donc sans leur consentement) éveille des craintes associées au développement insidieux d'une société de surveillance dans laquelle le pouvoir de gérer la divulgation de ses propres renseignements personnels, et donc l'autonomie des personnes, s'érode peu à peu[197].

En matière de vidéosurveillance, le consentement n'est tout simplement pas applicable. En fait, la seule manière pour les citoyens de ne pas consentir à la vidéosurveillance est d'éviter les endroits surveillés à l'aide de caméras[198]. Étant donné que les caméras de surveillance sont désormais largement répandues, tant dans les espaces publics que privés, une telle avenue semble impossible à explorer.

Plusieurs organismes se sont déjà prononcés sur la question du consentement à l'identification par radiofréquence. Le Groupe de l'article 29 a passé la technologie de l'IRF au crible de la *Directive* européenne en matière de protection des données personnelles. Le Groupe rappelle le rôle primordial que joue le consentement sur le plan légal lorsqu'il est question de l'IRF : « Dans la plupart des scénarios où est utilisée la technologie RFID, le consentement des personnes sera le seul motif légal que pourront invoquer les responsables du traitement des données pour légitimer la collecte d'informations par radio-identification. [...][199] ».

194. COMITÉ CONSULTATIF NATIONAL D'ÉTHIQUE POUR LES SCIENCES DE LA VIE ET DE LA SANTÉ, *op. cit.*, p. 17.

195. David H. FLAHERTY, *op. cit.*, p. 6.

196. ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, *op. cit.*, p. 5.

197. John D. WOODWARD Jr. *et al.*, *Army Biometric Applications : Identifying and Addressing Sociocultural Concerns*, RAND, 2001, p. 25. [http://www.rand.org/publications/MR/MR1237/].

198. Leon HEMPEL et Eric TOPFER, *op. cit.*, p. 66.

199. GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL DU PARLEMENT EUROPÉEN ET DU CONSEIL, *op. cit.*, p. 11.

La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels prévoit déjà que :

> *quiconque, au nom d'un organisme public, recueille verbalement un renseignement personnel auprès de la personne concernée doit se nommer et, lors de la première collecte de renseignements et par la suite sur demande, l'informer :*
>
> *1° du nom et de l'adresse de l'organisme public au nom de qui la collecte est faite ;*
>
> *2° des fins pour lesquelles ce renseignement est recueilli ;*
>
> *3° des catégories de personnes qui auront accès à ce renseignement ;*
>
> *4° du caractère obligatoire ou facultatif de la demande ;*
>
> *5° des conséquences pour la personne concernée ou, selon le cas, pour le tiers, d'un refus de répondre à la demande ;*
>
> *6° des droits d'accès et de rectification prévus par la loi*[200].

Par ailleurs, il faut rappeler, particulièrement dans le contexte du déploiement des NTSC à des fins de sécurité, que cet article est sujet à des restrictions : « Le présent article ne s'applique pas à une enquête de nature judiciaire, ni à une enquête ou à un constat faits par un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois[201]. »

Le Québec a tout de même prévu une disposition à l'égard du consentement à la biométrie. Dans son *Document de réflexion* sur l'utilisation des données biométriques, la Commission de l'éthique de la science et de la technologie traite de cet aspect :

> *L'article 44 de la Loi concernant le cadre juridique des technologies de l'information stipule [sic] que toute vérification ou confirmation de l'identité d'une personne au moyen de mesures biométriques ne peut se faire sans son « consentement exprès ». Il convient cependant de souligner que même le consentement d'une personne à la prise de mesures biométriques ne permet pas de passer outre à l'obligation de nécessité (c'est-à-dire que ce type d'information soit jugé nécessaire) prévue à l'article 64 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et aux articles 4 et 5 de la Loi sur la protection des renseignements personnels dans le secteur privé. En d'autres termes, il est interdit à un organisme public de recueillir une donnée biométrique si cette donnée n'est pas nécessaire à l'exercice de ses fonctions ou à la mise en œuvre d'un programme dont il a la gestion. L'obtention d'un consentement ne permet pas de contourner cette interdiction. Il en va de même pour une entreprise du secteur privé qui ne peut recueillir que les seules données qui sont nécessaires à l'objet du dossier constitué sur une personne*[202].

Dans le cadre de la Loi sur la protection des renseignements personnels dans le secteur privé, le consentement est balisé de la sorte : « Le consentement à la collecte, à la communication ou à l'utilisation d'un renseignement personnel doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Ce consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé[203]. »

De plus, l'article 8 prévoit que :

> *La personne qui recueille des renseignements personnels auprès de la personne concernée doit, lorsqu'elle constitue un dossier sur cette dernière, l'informer :*
>
> *1° de l'objet du dossier ;*
>
> *2° de l'utilisation qui sera faite des renseignements ainsi que des catégories de personnes qui y auront accès au sein de l'entreprise ;*
>
> *3° de l'endroit où sera détenu son dossier ainsi que des droits d'accès ou de rectification*[204].

En ce qui a trait à la communication des renseignements personnels, les articles 67, 67.1, 67.2, 68 et 68.1 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels sont autant de dérogations à l'obligation d'obtenir le consentement des personnes pour communiquer des renseignements personnels à leur sujet.

200. L.R.Q., chapitre A-2.1, 1982, c. 30, a. 65 ; 1990, c. 57, a. 15 ; 2006, c. 22, a. 36.

201. *Ibid.*

202. COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE, *L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques*, Document de réflexion, Sainte-Foy, 2005, p. 44.

203. L.R.Q., chapitre P-39.1, 1993, c. 17, a. 14 ; 2006, c. 22, a. 115.

204. L.R.Q., chapitre P-39.1, 1993, c. 17, a. 8.

Par exemple, l'article 68 prévoit que :

> *[un] organisme public peut, sans le consentement de la personne concernée, communiquer un renseignement personnel :*
>
> *1° à un organisme public ou à un organisme d'un autre gouvernement lorsque cette communication est nécessaire à l'exercice des attributions de l'organisme receveur ou à la mise en œuvre d'un programme dont cet organisme a la gestion ;*
>
> *1.1° à un organisme public ou à un organisme d'un autre gouvernement lorsque la communication est manifestement au bénéfice de la personne concernée ;*
>
> *2° à une personne ou à un organisme lorsque des circonstances exceptionnelles le justifient ;*
>
> *3° à une personne ou à un organisme si cette communication est nécessaire dans le cadre de la prestation d'un service à rendre à la personne concernée par un organisme public, notamment aux fins de l'identification de cette personne.*

De telles dispositions juridiques ouvrent la porte à la communication de renseignements personnels sans que la personne concernée soit mise au courant. Une fois le consentement obtenu pour la collecte de renseignements personnels par les NTSC, ces informations peuvent être communiquées à plusieurs acteurs sans le consentement des personnes concernées et ainsi à l'encontre du respect de son autonomie. Bien que des conditions doivent être remplies à cet effet, certaines demeurent suffisamment vagues pour ouvrir la porte à des abus.

Le caractère invisible du déploiement des NTSC, et ce, dans plusieurs dimensions de la vie quotidienne, est également une source de préoccupation. L'objectif de plusieurs promoteurs des NTSC est d'ailleurs d'intégrer ces technologies dans l'environnement en les camouflant. Cette façon de faire peut avoir des répercussions sur l'autonomie des citoyens et sur le respect de leur vie privée.

Si le consentement individuel ne s'applique pas au domaine des NTSC, il n'en demeure pas moins que l'autonomie des citoyens et, par le fait même, les valeurs fondamentales des sociétés démocratiques peuvent être privilégiées. Dans l'esprit du principe de représentativité, en vertu duquel ce sont des élus qui prennent les décisions politiques et non l'ensemble des citoyens, la Commission estime que, si le déploiement des NTSC se fait de manière transparente et en accord avec les valeurs fondamentales des sociétés démocratiques, chaque individu n'a pas nécessairement à donner son consentement. Il est cependant essentiel de réunir certaines conditions permettant d'éclairer le processus menant au déploiement des NTSC et de donner toute la marge de manœuvre nécessaire aux opposants et aux critiques afin que ceux-ci puissent exprimer leur point de vue. De plus, des mécanismes devraient être mis en place qui permettraient de consulter des groupes ou des populations qui seraient sujets à surveillance dans le cadre de projets bien précis.

Les informations qui doivent être données par les organismes publics et privés constituent un minimum. Sur le plan éthique, et à l'égard des NTSC, elles se révèlent toutefois insuffisantes pour contribuer à éclairer les décisions et les débats publics en la matière. Aussi, la Commission estime nécessaire que les citoyens soient mieux informés notamment et non exclusivement à l'égard des points suivants :

- les dispositions juridiques entourant le déploiement des NTSC, la collecte, l'utilisation, la communication et la conservation des renseignements personnels ;
- les risques, les inconvénients, les avantages et les bénéfices potentiels entraînés par le déploiement des NTSC ;
- les lieux et les documents soumis à la surveillance ;
- les moyens mis à la disposition des citoyens pour qu'ils participent au déploiement des NTSC, ce qui favoriserait un processus ouvert et transparent[205] ;
- les moyens mis à la disposition des citoyens pour faire connaître leur opinion en la matière, voire leurs plaintes, que ce soit sur le déploiement des NTSC en général ou sur un projet de déploiement de NTSC en particulier.

205. La Commission s'inspire ici des travaux de la Commissaire à la vie privée de l'Ontario en matière d'IRF. Voir Ann CAVOUKIAN, *Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines!)*, Information and Privacy Commissioner/Ontario, juin 2006, p. 2. [www.ipc.on.ca/images/Resources/up-rfidgdlines.pdf]

Le respect des finalités : un principe à réaffirmer

Le respect des finalités explicitées pour lesquelles les NTSC sont déployées et l'exploitation de toutes les utilisations possibles de ces dernières sont source de tensions. D'une part, le respect des finalités explicitées est un principe important qui tend à prévenir les détournements d'usage et certaines formes d'abus et de dérives. D'autre part, l'exploitation de toutes les utilisations possibles des NTSC (y compris des fins auxquelles les personnes n'ont pas consenti) permettrait probablement d'accroître la sécurité.

Cette problématique attire l'attention sur le phénomène de détournement d'usage, un risque appréhendé que l'Organisation de coopération et de développement économiques (OCDE) définit ainsi :

> *Le détournement d'usage est l'expression utilisée pour décrire le détournement d'un processus ou système, par lequel les données collectées pour une utilisation spécifique servent ensuite un autre objectif involontaire ou non autorisé. Du point de vue des principes régissant la protection de la vie privée, un tel détournement pourrait être considéré comme contraire au « principe de la spécification des finalités » puisqu'il équivaut à l'utilisation, la rétention ou la divulgation ultérieures de données sans le consentement de la personne et incompatibles avec le type d'utilisation spécifié au moment de leur collecte. Prenons l'exemple du système d'un service d'aide sociale qui impose une capture de l'empreinte des doigts au moment de l'inscription. Supposons que ce service se soit engagé auprès de l'allocataire inscrit à n'utiliser cette capture qu'à la seule fin de vérifier que ce dernier ne touche pas deux fois les prestations sociales (cumul d'avantages). Si la capture sert ensuite un autre objectif (par exemple une utilisation non décrite dans l'engagement initial), alors il s'agit d'un cas de détournement de type « function creep »*[206]

Devant les exemples portés à son attention, la Commission s'inquiète des glissements qu'elle observe et de ceux qui risquent de se produire dans un avenir rapproché. Des normes, des procédés, des pratiques, des moyens de surveillance et de contrôle mis en place dans la foulée d'attentats terroristes sont progressivement intégrés à la lutte à la petite délinquance, puis ils sont récupérés par le secteur commercial. À l'inverse, des technologies, comme l'IRF, dont les applications sont souvent associées au commerce de détail et à la gestion des inventaires semblent vouloir coloniser le domaine de la sécurité. Aussi, considérant la facilité avec laquelle les NTSC trouvent des applications et donc les finalités qui peuvent être très différentes, il convient de rester vigilant à cet égard.

Des préoccupations en lien avec le cadre normatif

À l'article 65 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, il est prévu que « quiconque, au nom d'un organisme public, recueille verbalement un renseignement personnel auprès de la personne concernée doit se nommer et, lors de la première collecte de renseignements et par la suite sur demande, l'informer [...] des fins pour lesquelles ce renseignement est recueilli[207] ». L'article 65.1 vient cependant limiter la portée de cet article lorsqu'il prévoit que :

> *l'organisme public peut toutefois utiliser un tel renseignement à une autre fin avec le consentement de la personne concernée ou, sans son consentement, dans les seuls cas suivants :*
>
> *1° lorsque son utilisation est à des fins compatibles avec celles pour lesquelles il a été recueilli ;*
>
> *2° lorsque son utilisation est manifestement au bénéfice de la personne concernée ;*
>
> *3° lorsque son utilisation est nécessaire à l'application d'une loi au Québec, que cette utilisation soit ou non prévue expressément par la loi*[208].

Cette dernière condition semble ouvrir la porte à une utilisation relativement ouverte des renseignements personnels, et ce, sans égard aux finalités pour lesquelles ils ont été recueillis dans un premier temps. En bref, si la collecte des renseignements personnels par l'entremise des NTSC est relativement bien restreinte aux finalités explicitées, l'utilisation de ces mêmes renseignements semble pouvoir facilement échapper à la règle du respect des finalités. Du point de vue éthique, la Commission estime qu'il s'agit là d'une source de préoccupation à l'égard du principe de respect des finalités et, par là même, quant au respect de l'autonomie des personnes.

206. ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, *op. cit.*, p. 13.

207. L.R.Q., chapitre A-2.1, 1982, c. 30, a. 65; 1990, c. 57, a. 15.

208. Ibid.

Des préoccupations en lien avec les différentes NTSC

La prolifération des banques de données de toutes sortes soulève des craintes relativement au détournement d'usage. Ces banques peuvent être piratées, vendues, cédées, et il subsiste un risque que ceux qui y ont accès en fassent un usage incompatible avec les fins visées. Certains observateurs ont fait remarquer que si les données biométriques se trouvent sur un support mobile, comme dans le cas d'une carte pouvant être conservée par l'usager, alors ce dernier risque moins que ses données fassent l'objet d'un détournement d'usage[209]. De fait, ses données ne se trouvent en aucun temps dans une banque de données et l'usager demeure en contrôle de la protection de ses propres données.

Dans le cas de la vidéosurveillance, le phénomène de détournement d'usage a été illustré avec éloquence lors de la 35e présentation du *Superbowl* à Tampa Bay en 2001. Les caméras de surveillance, mises en place pour effectuer une surveillance de type classique, ont été couplées à un programme de reconnaissance faciale. L'objectif de l'exercice était simple : comparer les visages captés dans la foule avec les photos de criminels recherchés[210]. La Commission désire exprimer son inquiétude quant à ce genre de pratique, d'autant plus que la fiabilité des systèmes actuels de reconnaissance faciale est loin d'être démontrée, car cette technique génère habituellement beaucoup de fausses associations. Pour faire une évaluation éthique adéquate de ce genre de détournement d'usage, il faut garder à l'esprit les promesses engendrées par ce genre de technologie, mais aussi les inconvénients et les risques qui lui sont associés. Des personnes identifiées à tort comme des étant des terroristes risquent de subir des préjudices, se retrouvant dans une situation où il leur faudra prouver leur innocence.

La Commission est d'autant plus préoccupée par le phénomène de détournement d'usage que les NTSC ont tendance, avec le développement de la technologie, à devenir de plus en plus discrètes. À cet égard, l'exemple des étiquettes d'IRF est éloquent. Ces dernières sont susceptibles de trouver une utilité dans une multitude de domaines et elles peuvent transmettre de l'information à distance, et ce, à l'insu même de ceux qui les portent. La dispersion des puces dans les objets de la vie quotidienne pourrait faire en sorte que de nombreuses informations personnelles s'y retrouvent éventuellement. Qui plus est, ces informations seraient accessibles à quiconque arriverait à les lire.

Les informations personnelles contenues dans les puces pourront dès lors servir aussi bien à mieux connaître le profil d'un consommateur, à certifier l'identité du détenteur d'un passeport qu'à connaître le dossier médical d'un patient inconscient. Pour bien comprendre comment les détournements d'usage peuvent avoir des répercussions inattendues et inquiétantes dans le domaine de la sécurité, il peut être pertinent de donner un exemple. Ainsi, une puce d'IRF implantée dans les passeports électroniques (ce qui est en voie de devenir la norme) contenant des informations biométriques, mais également des renseignements sur la nationalité de son détenteur, pourrait être lue par des lecteurs « non autorisés ». La Commission faisait référence à ce phénomène lorsqu'elle parlait plus haut de repérage clandestin : une personne non autorisée pourrait lire à distance le contenu de la puce, et ce, à l'insu du porteur de la puce[211]. En matière de sécurité, et dans le contexte actuel où les terroristes cherchent à cibler leurs attaques, le repérage clandestin pourrait servir à des terroristes désireux de « trier » leurs victimes éventuelles dans une foule selon leur nationalité, par exemple[212].

209. PORTUGUESE DATA PROTECTION AUTHORITY, *Principles for the Use of Biometric Data in Controlling Access and Monitoring Hours Worked*, Portugal, 26 février 2004, [http://www.cnpd.pt/english/bin/guidelines/Guidelines%20biometric%20(EN).HTM] ; GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL DE L'UNION EUROPÉENNE, *Document de travail sur la biométrie*, Bruxelles, Belgique, 1er août 2003, p. 6 et 7.

210. Philip E. AGRE, « Your Face Is Not a Bar Code : Arguments against Automatic Face Recognition in Public », [en ligne], 10 septembre 2003, [http://polaris.gseis.ucla.edu/pagre/bar-code.html].

211. GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL DU PARLEMENT EUROPÉEN ET DU CONSEIL, *Document de travail sur les questions de protection des données liées à la technologie RFID (radio-identification)*, Bruxelles, 19 janvier 2005, p. 8, [http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_fr.pdf].

212. *Ibid.*

Des préoccupations en lien avec la conservation des données

La durée de conservation des données collectées par les NTSC constitue un paramètre important dans les risques de détournement d'usage[213]. Le principe est simple : moins longtemps les données sont conservées, moins les risques de détournement d'usage sont grands. Par conséquent, il est important de prévoir la durée de conservation des enregistrements avant la mise en place d'un système de surveillance et cette durée ne doit pas excéder la durée normale de conservation nécessaire dans le cadre de la fin visée.

Enfin, il faut rappeler que le stockage centralisé de renseignements personnels accroit également le risque que ces données soient utilisées dans le but de dresser un profil détaillé des habitudes d'une personne. La question de la compatibilité des finalités pose également le problème de l'interopérabilité de différents systèmes reposant sur les NTSC. La standardisation qu'exige l'interopérabilité pourrait entrainer une plus forte interconnexion entre les bases de données et ainsi accentuer les risques d'abus et de dérives associés au détournement d'usage[214].

Des préoccupations en lien avec les risques de discrimination et de stigmatisation

L'analyse des renseignements personnels recueillis par les NTSC comporte des risques en matière de discrimination et de stigmatisation. Étant donné la nature des renseignements personnels recueillis et la possibilité d'en extraire des informations sur l'origine ethnique et sur la santé des usagers, sur leurs habitudes de consommation et leur affiliation avec des partis politiques, la question des risques de discrimination et de stigmatisation se pose avec acuité. En effet, dans le contexte de la lutte au terrorisme, par exemple, les données biométriques, les images captées par des caméras de surveillance, de même que les données recueillies par des systèmes d'IRF, risquent de conduire au « ciblage » de certaines catégories de personnes, ces dernières pouvant à la limite être victimes de discrimination et de stigmatisation[215]. En ce qui a trait à la vidéosurveillance, des études montrent que les personnes qui font l'objet d'une attention particulière par les opérateurs de ces systèmes sont plus souvent des hommes d'origine étrangère[216]. De plus, la question de savoir quelle personne ou quelles catégories d'individus doivent être ciblées par la vérification de leur identité est généralement laissée à la discrétion de la police. Bien que les systèmes de surveillance ne soient pas mis en place dans le but de créer de la discrimination et de la stigmatisation, la Commission considère qu'il s'agit d'un détournement d'usage aussi vraisemblable qu'inacceptable.

* * *

Malgré tout, les NTSC offrent un potentiel très intéressant en matière de surveillance ainsi que pour l'évaluation et la gestion des risques sur le plan de la sécurité. Ce point ne doit être ni négligé ni sous-estimé. Si d'aucuns voient dans la popularité croissante des moyens de surveillance une menace pour les droits et libertés des citoyens dans une société démocratique, les plus optimistes feront valoir que ces mêmes moyens peuvent contribuer à la prévention de la criminalité, voire du terrorisme.

Bien qu'ils puissent servir la prévention du crime, les détournements d'usage posent des risques de dérives et d'abus qui commandent une grande attention. En donnant l'aval à l'exploitation de toutes les utilisations possibles des NTSC afin de protéger la démocratie et l'ordre public contre le terrorisme et les autres formes de criminalité, la Commission craint justement le sacrifice de droits et de libertés qui fondent la démocratie. La Commission insiste tout au long du présent avis sur la nécessité de trouver des équilibres et elle en vient à la conclusion que la démocratie elle-même constitue un

213. Terry HONESS et Elizabeth CHARMAN, *Closed Circuit Television in Public Places : Its Acceptability and Perceived Effectiveness*, Police Research Group, Crime prevention unit series : paper n° 35, Londres, Home Office Police Department, p. 15.

214. GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL DE L'UNION EUROPÉENNE, *Document de travail sur la biométrie*, Bruxelles, Belgique, 1er août 2003, p. 6 et 7.

215. COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE, *L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques*, Document de réflexion, Sainte-Foy, 2005, p. 44.

216. Gavin J.D. SMITH, « Behind the Screens : Examining Constructions of Deviance and Informal Practices among CCTV Control Room Operators in the UK », *Surveillance & Society*, vol. 2, n° 2/3, p. 385-387 ; Ann Rudinow SÆTNAN, Heidi Mork LOMELL et Carsten WIECEK, « Controlling CCTV in Public Spaces : Is Privacy the (Only) Issue? Reflections on Norwegian and Danish observations », *Surveillance & Society*, vol. 2, n° 2/3, p. 405-407.

équilibre toujours fragile entre la liberté et la répression. Elle estime que les NTSC peuvent faire beaucoup pour améliorer la sécurité du public, mais qu'il n'est pas toujours nécessaire d'exploiter toutes les utilisations possibles leur étant associées pour assurer un niveau acceptable de sécurité.

La protection des renseignements personnels : pour des conduites respectueuses de la vie privée

La question des NTSC est souvent ramenée à un seul enjeu : la protection des renseignements personnels. Cette importance est notamment due au fait que les NTSC sont principalement déployées pour recueillir des renseignements (qui sont souvent personnels). Cet enjeu, plus que tout autre, concerne les valeurs de respect de la vie privée et de sécurité. Si les renseignements personnels en disent long sur la vie privée des personnes, ils sont souvent vus comme une source riche d'informations permettant d'améliorer la sécurité.

Les nouvelles technologies de l'information et des communications peuvent autant protéger les renseignements personnels que faciliter l'accès et le partage à ces mêmes données. Les technologies de chiffrement, par exemple, peuvent aussi bien servir à sécuriser la communication entre deux interlocuteurs qu'à donner l'impression qu'elle est privée, alors qu'elle est interceptée[217]. Dans le contexte actuel, le respect de la vie privée est un objet de préoccupation pour une autre raison. Le nombre grandissant de banques de données mises en place par des organismes, tant publics que privés, constitue à lui seul un phénomène qui mérite l'attention. Ces assemblages de renseignements personnels ne sont pas étrangers aux besoins de la société du risque. Aussi utiles puissent-elles être pour les organisations dans la gestion du risque en matière de sécurité, les bases de données contenant des renseignements personnels de cette envergure posent des défis majeurs en matière de protection de la confidentialité et de l'utilisation à des fins autres que celles prévues à l'origine.

La protection des renseignements personnels est presque systématiquement associée au respect de la vie privée. Il est vrai que les renseignements dits personnels ouvrent une fenêtre sur divers aspects de notre vie privée. En fait, la protection des renseignements personnels constitue un moyen d'actualiser la valeur de la vie privée. Si la première est davantage un concept juridique, le respect de la vie privée, dans le cadre du présent avis doit être entendu comme une valeur.

Les données recueillies par des systèmes biométriques, par la vidéosurveillance et par l'IRF sont presque systématiquement des renseignements personnels. Par conséquent, le degré de respect de la vie privée des personnes objets de la surveillance variera en fonction de l'utilisation, de la communication et de la conservation qui seront faites de ces données.

Chacune des NTSC abordées dans le cadre du présent avis établit son propre rapport avec les renseignements personnels. De plus, chacune a un potentiel d'intrusion dans la vie privée qui est différent. C'est pourquoi la Commission a examiné les liens qui unissent le déploiement des NTSC, le respect de la vie privée et la protection des renseignements personnels en abordant tour à tour chacune des NTSC.

Données biométriques

La question de la protection des renseignements personnels est indissociable des systèmes biométriques, car les mesures biométriques sont considérées comme des renseignements personnels. Le fait que certaines données biométriques constituent des « identifiants intimes bavards[218] » explique probablement pourquoi les systèmes biométriques font parfois craindre le pire en ce qui a trait au respect de la vie privée des personnes. Les données biométriques peuvent être qualifiées d'identifiants intimes du fait qu'elles sont étroitement liées à l'individu auquel elles se rapportent. Le caractère bavard de certains identifiants biométriques constitue également un objet d'inquiétude : les données biométriques portent en elles-mêmes plus d'informations que la simple reproduction de l'image d'une empreinte digitale, par exemple. En effet, selon certains

217. UNESCO, *op. cit.*, p. 14.

218. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *La biométrie au Québec : les enjeux*, Document d'analyse, juillet 2002, p. 25.

experts, il est même possible de récolter des informations sur l'état de santé ou encore sur l'humeur des individus seulement par l'analyse des empreintes digitales ou encore de la rétine[219]. Les personnes préfèrent généralement que certaines informations qui sont en leur possession et qui les concernent personnellement demeurent confidentielles ou, du moins, qu'elles soient traitées comme telles[220].

En principe, seules les personnes autorisées à accéder aux renseignements personnels y accéderont effectivement. Un problème peut toutefois se poser lorsqu'une personne exerce son droit d'accès à l'information colligée ou de rectification de cette information (articles 83 et 89 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, articles 27 et 28 de la Loi sur la protection des renseignements personnels dans le secteur privé et article 40 du Code civil[221]), en raison du processus de numérisation appliqué à l'information brute qui rend celle-ci visuellement indéchiffrable[222]. Il devient dès lors quasi impossible de vérifier l'authenticité et la qualité de la « signature », ce que toute personne peut faire dans le cas de son dossier de crédit, par exemple quand elle veut s'assurer que son contenu est à jour et conforme à la réalité.

Selon des experts de l'industrie, la biométrie n'est pas en soi une technologie intrusive et elle peut être utilisée de façon efficace pour réduire les atteintes à la vie privée[223]. Selon eux, il ne faut pas nécessairement sacrifier la vie privée pour garantir la sécurité et vice versa et, en principe, les deux peuvent bénéficier d'une utilisation transparente et légitime d'un système biométrique bien conçu.

La Commission d'accès à l'information a quant à elle défini les liens entre la sécurité et la vie privée dans le contexte de l'utilisation des données biométriques :

> *En fait, bien que la plupart des techniques biométriques soient des outils de sécurité fort efficaces, ils ne brillent pas par leur innocuité en ce qui concerne la protection de la vie privée des personnes qui les utilisent. Il faut ici faire clairement la distinction entre le concept de sécurité et celui de protection de la vie privée et des renseignements personnels; il n'est pas rare que des mécanismes de sécurité atteignent à la vie privée des personnes qui les utilisent, comme la Commission d'accès à l'information l'a déjà démontré dans un avis récent sur l'infrastructure à clés publiques gouvernementale. Ces atteintes à la vie privée concernent la collecte supplémentaire de renseignements personnels pour faire fonctionner le système de sécurité, le traitement de ces renseignements et la possibilité de traçage et de constitution de profils*[224].

Les répercussions sur la vie privée dépendent non pas de la technologie elle-même, mais de la façon dont celle-ci est utilisée. En outre, dans un système conçu pour l'authentification des personnes (donc pour savoir si la personne est bien celle qu'elle prétend être), un stockage décentralisé de l'information est généralement suffisant. Mais dans une perspective d'identification (donc pour savoir qui est cette personne), notamment en matière judiciaire, le processus repose sur le balayage de données centralisées dans une ou plusieurs bases de données. Certains experts en sécurité admettent que les bases de données centralisées constituent un risque en soi[225]; en outre, en ce qui concerne les données biométriques conservées sur un support portable, les possibilités de vol du support et de la capture d'information à l'insu des utilisateurs doivent être envisagées[226].

Il apparaît important de souligner que les systèmes biométriques sont des systèmes informatiques autonomes ou installés en réseaux. Lorsqu'elles sont stockées dans une mémoire centralisée et non pas sur un disque dur ou sur

219. INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES, *Sécurité et respect de la vie privée du citoyen à l'ère du numérique après le 11 septembre. Vision prospective, document de synthèse*, Commission européenne, juillet 2003, p. 50-54.

220. Ann CAVOUKIAN, *Biometrics and Policing: Comments from a Privacy Perspective*, Information and Privacy Commissioner/Ontario, août 1999, p. 10.

221. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *La biométrie au Québec : les enjeux*, Document d'analyse, juillet 2002, p. 37.

222. OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, *op. cit.*, 2e partie, p. 21 et 22.

223. CITOYENNETÉ ET IMMIGRATION CANADA, « Biométrie : incidences et applications pour la citoyenneté et l'immigration », document d'information, Forum tenu les 7 et 8 octobre 2003, Ottawa, Canada, p. 19.

224. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *La biométrie au Québec : les enjeux*, Document d'analyse, juillet 2002, p. 23.

225. *Ibid.*, p. 30.

226. *Ibid.*, p. 33.

une micropuce, les données biométriques « voyagent » et peuvent être couplées avec des données présentes dans d'autres bases de données ayant en mémoire d'autres types d'informations sur les mêmes personnes. Se crée ainsi un profil de plus en plus complet d'une personne au fur et à mesure que les renseignements la concernant s'apparient. Autre possibilité, plus l'information s'« enrichit » et plus la base de données s'élargit, plus s'excite la convoitise des pirates informatiques qui chercheront à profiter de façon malveillante et mercantile des « nombreuses vulnérabilités de ces réseaux, des logiciels qui les soutiennent et des bases de données[227] » qu'ils contiennent.

Heureusement, comme l'observe la CAI, la loi québécoise ne permet pas aux organismes de partager l'information recueillie sur les personnes, sauf dans certaines circonstances, et encourage un cloisonnement de l'information susceptible de protéger la vie privée[228]. Toutefois, dans un contexte où la centralisation et l'intégration des systèmes d'information constituent un atout sur le plan économique et en matière d'accès à l'information par un plus grand nombre de personnes, il y a un risque accru que l'État souhaite tirer profit de cette mine d'information à toutes sortes de fins, bénéfiques ou non pour la société dans son ensemble ou pour certains segments de la population particulièrement vulnérables.

Vidéosurveillance

Par son caractère invisible et distant, la vidéosurveillance peut représenter une menace pour la vie privée. En effet, la technologie permet de filmer des personnes à leur insu, et ce, tant dans des lieux publics que dans des endroits privés. Or, lorsqu'elle circule dans des lieux publics, une personne doit admettre qu'elle ne bénéficie pas de la même intimité que dans sa maison, par exemple. Toutefois, ce serait abuser de ce principe que de prétendre que la personne renonce totalement au respect de sa vie privée dans les lieux publics. Toute personne est aussi en droit de circuler dans des lieux publics sans être constamment l'objet d'une surveillance. Le respect de sa vie privée s'applique, et ce, même dans des lieux publics.

Identification par radiofréquence

L'Europe fait figure de pionnière en ce qui a trait à la réflexion à propos des enjeux liés à la protection des renseignements personnels et à la vie privée que pose l'IRF. L'encadré suivant décrit la problématique, résumée en quelques mots par le Groupe de l'article 29.

La vie privée et la protection des renseignements personnels dans le cas de l'IRF pour le Groupe de l'article 29

Tandis que les avantages liés à l'utilisation de la technologie RFID paraissent évidents, le vaste déploiement de cette technologie n'est pas sans comporter des inconvénients potentiels. Sur le front de la protection des données, le groupe de travail de l'article 29 se préoccupe de la possibilité pour certaines applications de la technologie RFID de porter atteinte à la dignité humaine et aux droits en matière de protection des données. En particulier, d'aucuns redoutent que des entreprises et des gouvernements puissent utiliser la technologie RFID pour fouiller dans la vie privée des personnes. La possibilité de collecter subrepticement diverses données toutes liées à la même personne; de suivre à la trace des personnes se déplaçant dans des lieux publics (aéroports, gares ferroviaires, magasins); d'étoffer des profils en surveillant le comportement des consommateurs dans les magasins, de lire les données détaillées des vêtements et des accessoires que portent les clients et des médicaments qu'ils transportent sont autant d'exemples d'utilisation de la technologie RFID qui suscitent des inquiétudes en matière de protection de la vie privée. Le problème est aggravé par le fait que, en raison de son coût relativement faible, cette technologie sera à la portée non seulement d'acteurs de premier plan mais aussi d'éléments de moindre rang et de simples citoyens[229].

À cela il faut ajouter l'analyse d'un commissaire de la Commission nationale de l'informatique et des libertés (CNIL) concernant les pièges « qui concourent à minorer le risque que présente cette technologie en matière de protection des données personnelles et de la vie privée[230] ». Selon lui, l'IRF, du fait de ses caractéristiques, risque de faire passer sous silence l'enjeu du respect de la vie privée :

227. *Ibid.*, p. 30.

228. *Ibid.*, p. 26.

229. GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL DU PARLEMENT EUROPÉEN ET DU CONSEIL, *Document de travail sur les questions de protection des données liées à la technologie RFID (radio-identification)*, Bruxelles, 19 janvier 2005, p. 2. [http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_fr.pdf].

230. COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, « La radio-identification », *cnil.fr* [en ligne], 30 juin 2006. [http://www.cnil.fr/index.php?id=1063].

- *l'insignifiance [apparente] des données;*
- *la priorité donnée aux objets [en apparence toujours vis-à-vis des personnes];*
- *la logique de mondialisation [normalisation technologique basée sur un concept américain de « privacy » sans prise en compte des principes européens de protection de la vie privée];*
- *et enfin le risque de « non-vigilance » individuelle [présence et activation invisibles]*[231].

Tout comme la vidéosurveillance, l'IRF peut s'avérer une méthode subreptice de surveillance et être utilisée pour suivre des personnes à la trace. C'est pourquoi les commentaires de la Commission au sujet de la vidéosurveillance s'appliquent aussi dans le cas de l'IRF. Cependant, la nature des renseignements personnels recueillis est différente. Dans le cas de la vidéosurveillance, ce sont les images captées et donc possiblement le visage des personnes qui seront les renseignements personnels. Pour l'IRF, des renseignements personnels cruciaux sont susceptibles d'être recueillis et utilisés : informations sur le crédit, la santé, l'identité, la nationalité, etc. La nature de ces renseignements pose donc des risques accrus d'atteinte à la vie privée des citoyens.

Pour le moment, la principale application de l'IRF consiste à introduire des données biométriques dans des puces qui sont à leur tour incorporées à des passeports. L'objectif de cette application est de rendre la contrefaçon plus difficile pour des individus mal intentionnés et de réduire les risques de vol d'identité. Mais il faut savoir que les systèmes en place ne protègent pas les informations contenues dans les puces par un procédé de chiffrement. Il a été démontré qu'au moyen d'un équipement rudimentaire, il est possible de dupliquer la puce d'IRF contenant des informations biométriques et de forger un nouveau passeport identique à l'original[232]. En outre, cette absence de chiffrement pourrait permettre l'interception de l'information lorsqu'elle est lue par un lecteur au moment du contrôle de l'identité. En d'autres mots, les données inscrites sur la puce pourraient être captées lorsqu'elles sont en transit, et ce, par un lecteur non autorisé. Enfin, la lecture de documents d'identité à divers « points de service » pourrait aussi permettre de suivre à la trace les détenteurs de ces documents.

Partant de là, trois types de risques pèsent sur le respect de la vie privée[233]. Le premier type de risques est associé à la collecte d'informations qui peuvent être directement ou indirectement liées à des renseignements personnels. Bien entendu, ce type de risques n'est pas propre à l'IRF. Le deuxième type de risques se présente lorsque des renseignements personnels sont stockés sur des puces d'IRF, comme c'est le cas dans certains passeports qui contiennent une empreinte digitale numérisée, par exemple. Enfin, le troisième type de risques se pose lorsque l'IRF permet la traçabilité des personnes. De fait, si les étiquettes sont associées à des renseignements personnels, la lecture de l'étiquette par des lecteurs, autorisés ou non, confirme la présence d'une personne identifiable à l'endroit et au moment de la lecture.

Pour tenter de contrecarrer ces risques, un certain consensus émerge autour de l'utilisation de technologies favorisant la vie privée (ou *privacy enhancing technologies*) dans la conception de la technologie d'IRF. À ce sujet, la Commissaire à l'information et à la vie privée de l'Ontario recommande que le souci de préserver le plus possible la vie privée des personnes doit faire partie intégrante du développement des technologies d'IRF, et ce, dès les premières étapes de conception[234]. Puisque les nouveaux passeports des citoyens de la plupart des membres de l'Union européenne et ceux maintenant délivrés aux citoyens américains comportent une puce d'IRF et devant l'intérêt déjà manifesté par le gouvernement du Canada pour l'introduction de données biométriques dans les documents d'identité des citoyens canadiens, la Commission estime qu'il faut rapidement statuer sur la manière d'encadrer l'introduction de ces technologies dans les documents d'identité. En outre, les expériences européenne et américaine montrent l'importance de protéger les renseignements personnels de manière adéquate si l'objectif de sécurisation des documents d'identité doit être atteint. Pour sa part, et considérant les

231. *Ibid.*

232. Kim ZETTER, *op. cit.*

233. COMMISSION EUROPÉENNE, *RFID Security, Data Protection and Privacy, Health and Safety Issues*, Policy Framework Paper [en ligne], 11 mai 2006, p. 10. [http://www.rfidconsultation.eu/41/38/264.html].

234. Ann CAVOUKIAN, *Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines)*, Information and Privacy Commissioner/Ontario, juin 2006, p. 2. [www.ipc.on.ca/images/Resources/up-rfidgdlines.pdf].

risques élevés en matière de respect de la vie privée et de protection des renseignements personnels, la Commission estime important que le gouvernement du Québec travaille de concert avec les instances concernées au sein du gouvernement du Canada pour que, dans l'éventualité d'une introduction de puces d'IRF dans les documents d'identité des Canadiens, ces puces d'IRF contenant des renseignements personnels soient dotées d'un procédé de chiffrement qui permette de sécuriser les données et, ainsi, de mieux protéger la vie privée et d'assurer une meilleure protection des renseignements personnels.

Le traitement automatisé de l'information : une pratique qui soulève des inquiétudes

Dans son document de réflexion sur la biométrie, la Commission a aussi soulevé la question du traitement automatisé de l'information, une pratique qui n'est pas sans susciter des inquiétudes sérieuses et qui s'applique aux fins NTSC décrites dans le présent avis :

> *Sauf à plaindre, mais aussi sur d'autres aspects de l'information véhiculée par une donnée biométrique, il faut également considérer que des décisions concernant des personnes peuvent être prises de façon automatique par des systèmes informatisés, sur la seule base de l'information disponible. De telles décisions, prises à l'insu de la personne, et fondées sur une information utilisée hors contexte et sur des faits parfois incomplets, imprécis, non pertinents ou périmés, peuvent s'avérer préjudiciables à la personne concernée[1].*

Il serait inacceptable que des décisions basées sur des traitements automatisés deviennent monnaie courante dans le milieu de la surveillance et du contrôle de l'identité. La déshumanisation complète de la décision sécuritaire doit être évitée. Ici encore, il semble qu'un équilibre doit être atteint entre la part dévolue aux personnes et celle confiée à la machine en ce qui a trait à la surveillance et aux traitements des données recueillies. D'un côté, plus la part de gestion et d'administration des systèmes de surveillance est l'affaire de personnes, plus il faut s'attendre à ce que les expériences de vie de ces gestionnaires influent parfois sur leurs décisions. Mais il est inutile de se leurrer : personne n'est en mesure de faire totalement abstraction de ses opinions personnelles dans la conduite de son travail. D'autre part, si le traitement automatisé et informatisé des données peut réduire la part de l'influence des opinions et des préjugés des opérateurs de systèmes de surveillance, il n'en demeure pas moins inquiétant de savoir que des décisions préjudiciables peuvent alors être prises sur la base de ce traitement sans que qui que ce soit ait pu remettre en contexte les informations traitées.

Le transfert transfrontalier de renseignements personnels

Enfin, il faut se demander si le niveau de protection des renseignements personnels est le même d'un pays à l'autre et si le transfert de ces renseignements d'un pays doté de mesures favorisant largement la protection des données personnelles vers un pays qui n'a pas autant à offrir est acceptable. Déjà, les consommateurs traitent sur Internet avec des entreprises de l'extérieur du pays qui conservent des renseignements personnels à leur égard, sans qu'ils connaissent toujours la manière dont ces renseignements seront protégés. Or, dans ces cas, les consommateurs sont toujours libres de ne pas effectuer ce genre de transactions. Mais en ce qui concerne des renseignements obtenus par le moyen de NTSC, les personnes ne savent pas toujours que des renseignements personnels les concernant seront conservés. Manifestement, une telle perspective n'est pas sans poser la question du contrôle de l'individu sur la direction que peuvent prendre ses renseignements personnels.

* * *

Le présent avis met en lumière des questions auxquelles la Commission n'est pas en mesure de répondre et dont elle ne peut assurer le suivi. Toutefois, celle-ci estime que plusieurs actions doivent être entreprises pour apporter des solutions et que les acteurs gouvernementaux en mesure de les accomplir sont facilement identifiables.

Considérant que le ministre responsable des Affaires intergouvernementales canadiennes, des Affaires autochtones, de la Francophonie canadienne, de la Réforme des institutions démocratiques et de l'Accès à l'information a pour mandat de conseiller le gouvernement en lui fournissant des avis en matière d'accès à l'information et de protection des renseignements

personnels, notamment lors de la présentation de projets de loi ou de développement de systèmes d'information et qu'à cette fin il peut consulter la Commission d'accès à l'information ;

Considérant que la Commission d'accès à l'information est chargée d'assurer le respect et la promotion de l'accès aux documents et de la protection des renseignements personnels et qu'elle peut prescrire des conditions applicables à un fichier de renseignements personnels auxquelles l'organisme public doit se conformer ;

Considérant que la Commission d'accès à l'information peut également, au terme d'une enquête relative à la collecte, à la détention, à la communication ou à l'utilisation de renseignements personnels par une personne qui exploite une entreprise, après lui avoir fourni l'occasion de présenter ses observations, lui recommander ou lui ordonner l'application de toute mesure corrective propre à assurer la protection des renseignements personnels ;

Et considérant que la Commission des droits de la personne et des droits de la jeunesse du Québec a notamment pour mandats :

- d'élaborer et d'appliquer un programme d'information et d'éducation, tant en matière de droits de la personne que de protection des droits de la jeunesse ;
- de diriger et encourager les recherches et les publications sur les libertés et droits fondamentaux et sur les droits de la jeunesse ;
- de recevoir les suggestions, recommandations et demandes touchant les droits et libertés de la personne, en tenant des auditions publiques au besoin, et d'adresser au gouvernement les recommandations appropriées ;
- de coopérer avec toute organisation vouée à la promotion des droits et libertés de la personne, au Québec ou à l'extérieur,

la Commission recommande au ministre responsable des Affaires intergouvernementales canadiennes, des Affaires autochtones, de la Francophonie canadienne, de la Réforme des institutions démocratiques et de l'Accès à l'information, à la Commission d'accès à l'information et à la Commission des droits de la personne et des droits de la jeunesse du Québec de collaborer ensemble dans le but de mettre en œuvre les actions suivantes :

1. Favoriser le dialogue entre les citoyens, le gouvernement et l'industrie en vue d'adopter des lignes directrices pour l'utilisation de ces technologies qui tiennent compte des préoccupations éthiques en la matière et des valeurs fondamentales des sociétés démocratiques.
2. Suivant une approche consultative, conseiller le gouvernement dans ses projets de déploiement de NTSC, notamment sur les aspects soulevant des enjeux éthiques et à la lumière des critères de pertinence, d'efficacité et de fiabilité.
3. Organiser une consultation de la population (sur le modèle du forum citoyen élaboré par le Commissaire à la santé et au bien-être) qui ferait une place importante aux enjeux éthiques.
4. Diffuser les résultats de cette consultation dans la population afin de la sensibiliser aux questions d'éthique associées aux NTSC.
5. Informer la population quant aux dispositions juridiques entourant le déploiement des NTSC, à ses conséquences pour les valeurs d'autonomie, de liberté, de sécurité et de vie privée et aux moyens mis à la disposition des citoyens pour participer à la prise de décision, à la mise en œuvre et au suivi en la matière.
6. Mettre en place un mécanisme de réparation et de rectification pour les cas où l'utilisation des NTSC cause des préjudices à des personnes en les associant à tort à des activités illicites.

Conclusion

Viser un juste équilibre entre les valeurs fondamentales au sein des démocraties n'est pas une mince affaire, particulièrement lorsque certaines d'entre elles entrent en conflit. Le cas du déploiement des nouvelles technologies de surveillance et de contrôle (NTSC) en fournit une claire illustration. Le fait d'aborder des éléments contextuels tels que la place qu'occupe une préoccupation renouvelée pour la sécurité, le sentiment d'insécurité, le risque et la surveillance a permis un regard éthique dans une perspective plus large.

La Commission a tenu à expliciter le cadre éthique dans lequel elle situe son analyse. Avant de présenter plus en détail les différentes NTSC, elle décrit les valeurs en jeu et les enjeux éthiques. Par ailleurs, tout au long du processus menant à la publication de son avis, la Commission a réalisé à quel point la frontière entre les espaces privés et les espaces publics est floue. Et, durant ses travaux, la Commission a constaté que cette frontière se brouille de plus en plus. Cette observation a des répercussions sur le plan éthique, car elle signifie que l'importance accordée à la valeur de vie privée est de plus en plus matière à débat, sinon remise en question. La Commission estimait par ailleurs essentiel de présenter les divers instruments normatifs en place, tant à l'échelle québécoise, canadienne qu'internationale. Qui plus est, elle a accordé une attention spéciale à la définition juridique du concept de renseignement personnel, une notion centrale de son analyse.

Trois technologies ont fait l'objet du regard éthique de la Commission. Tour à tour, les systèmes biométriques, la vidéosurveillance et l'identification par radiofréquence (IRF) sont décrits afin de familiariser le lecteur avec ces technologies. Connaître et comprendre les finalités associées à l'utilisation de ces technologies, leurs applications actuelles et leur mode de fonctionnement, leurs atouts, leurs failles, mais aussi les tendances du marché et l'intérêt de la population constitue une étape incontournable. C'est pourquoi la Commission a consacré un chapitre complet à l'étude des NTSC. La consultation d'experts a permis de constater que ces technologies sont de plus en plus présentes dans la vie quotidienne. En outre, le marché de la sécurité est en pleine croissance et tente de répondre à un intérêt certain de la population. Comme toutes les technologies en émergence, les NTSC sont remplies de promesses, tant sur le plan de l'amélioration de la sécurité que sur le plan de la convivialité. Toutefois, ces technologies ne sont pas exemptes de failles.

Des enjeux éthiques soulevés par le déploiement des NTSC, six d'entre eux ont retenu l'attention de la Commission. À travers chacun d'eux, elle a tenté de ne pas privilégier une valeur par rapport à une autre de manière disproportionnée, l'objectif étant de parvenir à un juste équilibre.

Tout d'abord, la Commission s'est penchée sur l'évaluation de la pertinence, de l'efficacité et de la fiabilité des NTSC. Elle estime que, pour être légitimes dans leur déploiement, les NTSC doivent, dans un premier temps, être pertinentes, efficaces et fiables. Ayant constaté que les NTSC ne sont pas encore en mesure de remplir toutes leurs promesses, la Commission estime que la prudence s'impose en la matière. Le déploiement de technologies perçues comme fiables et qui contribueraient à répandre un faux sentiment de sécurité dans la population serait inacceptable. De plus, elle estime nécessaire de rappeler l'importance de déployer des technologies efficaces et fiables afin d'éviter de causer des préjudices à des personnes innocentes. Finalement, cet enjeu pose la question de la transparence du processus d'évaluation à l'endroit de la population.

Au regard de l'enjeu de la proportionnalité de la réponse à l'insécurité, la Commission s'est dite préoccupée par l'ampleur que pourrait prendre un déploiement des NTSC qui serait une réponse à la demande insatiable pour plus de sécurité. La mise en place de NTSC doit avoir pour objectif principal de chercher à atteindre un niveau jugé acceptable de sécurité, sans plus. Parce que chaque projet de déploiement de NTSC est différent à

plusieurs égards, l'évaluation du rapport entre la fiabilité technique, la proportionnalité de la réponse à l'insécurité et le degré d'intrusion dans la vie privée est à refaire à chaque fois. Pour réussir un déploiement en fonction de l'atteinte d'un niveau acceptable de sécurité, un dialogue entre les décideurs publics et privés doit s'engager. Chose certaine, la mise en place de moyens de surveillance trop intrusifs et la collecte de renseignements personnels qui ne sont pas nécessaires aux fins visées sont des pratiques inadmissibles, peu importe le projet. La Commission invite donc les décideurs politiques et privés à procéder à une évaluation et à une interprétation nuancées et lucides des besoins en matière de NTSC à des fins de sécurité. De plus, considérant que les fournisseurs et les installateurs sont souvent amenés à juger de la proportionnalité des moyens technologiques déployés en réponse à l'insécurité et qu'ils sont les premiers confrontés aux enjeux éthiques mentionnés par la Commission, il est nécessaire qu'ils soient sensibilisés à ces questions pour que le déploiement des NTSC se fasse en accord avec les valeurs privilégiées. C'est pourquoi la Commission recommande que la formation donnée par le Bureau de la sécurité privée aux représentants des titulaires de permis d'agence inclue un volet éthique obligatoire qui s'inspirera des enjeux éthiques soulevés dans le présent avis et que le gouvernement, conformément à la Loi sur la sécurité privée, adopte la réglementation nécessaire pour que la formation exigée pour la délivrance d'un permis d'agent prévoie également un tel volet éthique.

En ce qui a trait à l'enjeu de l'acceptabilité sociale, toute forme de consultation sur les NTSC doit faire une place importante à la population en général et chercher d'abord et avant tout à recueillir des opinions éclairées.

En raison de la nature même des NTSC, il est difficile, voire impossible d'obtenir un consentement individuel, libre et éclairé des personnes surveillées. L'enjeu du consentement pose donc de nombreux défis à cet égard. De plus, la Commission attire l'attention sur les limites des dispositions législatives encadrant le consentement à la collecte et à la communication des renseignements personnels. Aussi est-il nécessaire que les citoyens soient mieux informés à l'égard des dispositions juridiques entourant la collecte, l'utilisation, la communication et la conservation des renseignements personnels, à l'égard des risques, des inconvénients, des avantages et des bénéfices potentiels entraînés par le déploiement des NTSC, à l'égard des lieux et des documents soumis à la surveillance, de même qu'à l'égard des moyens mis à la disposition des citoyens pour participer au déploiement des NTSC, ce qui favoriserait un processus d'implantation de systèmes de sécurité ouvert, transparent et modifiable.

En matière de respect des finalités, la tension entre le respect des finalités explicitées pour lesquelles les NTSC sont déployées et l'exploitation de toutes les utilisations possibles de ces dernières constitue le cœur d'un autre enjeu éthique. De plus, certains facteurs comme la durée de conservation des renseignements personnels peuvent influer sur les risques de dérives et d'abus, notamment les risques de discrimination et de stigmatisation. Bien qu'elle reconnaisse que les NTSC peuvent faire beaucoup pour améliorer la sécurité du public, la Commission estime qu'il n'est pas toujours nécessaire d'exploiter toutes les utilisations possibles qui leur sont associées pour assurer un niveau acceptable de sécurité.

La protection des renseignements personnels constitue un moyen d'actualiser la valeur de la vie privée. Comme chacune des NTSC établit un rapport singulier avec cet enjeu, les systèmes biométriques, la vidéosurveillance et l'identification par radiofréquence font l'objet d'un traitement séparé. En matière de système biométrique, la Commission émet des réserves quant à la communication des renseignements personnels que sont les données biométriques et elle réitère sa préférence pour des systèmes où les usagers gardent un maximum de contrôle sur les données les concernant. Elle rappelle que les données biométriques sont des identifiants intimement associés à une personne (puisque les probabilités que deux personnes partagent certaines caractéristiques biométriques sont quasi nulles) et qu'elles peuvent révéler plus que l'identité de la personne. La Commission exprime également des inquiétudes relativement à l'aspect intrusif de la vidéosurveillance dans la vie privée. Enfin, en matière d'identification par radiofréquence, la Commission attire l'attention sur le fait que les données susceptibles d'être stockées sur les étiquettes d'IRF sont des renseignements personnels. De plus, l'introduction de ces étiquettes dans des documents d'identité, par exemple, fait poindre la possibilité de repérer les mouvements des personnes dans l'espace et dans le temps. Mais, encore plus préoccupant, les passeports dotés de telles puces se sont révélés faciles à falsifier. Considérant les risques imposants en matière de respect de la vie privée et de protection des renseignements personnels, la Commission estime important

que le gouvernement du Québec travaille de concert avec les instances concernées au sein du gouvernement du Canada pour que, dans l'éventualité d'une introduction de puces d'IRF dans les documents d'identité des Canadiens, ces puces d'IRF contenant des renseignements personnels soient dotées d'un procédé de chiffrement qui permettrait de sécuriser les données et, ainsi, de mieux protéger la vie privée et d'assurer une meilleure protection des renseignements personnels.

De plus, la Commission formule une mise en garde relative au phénomène de normativité clandestine à l'œuvre dans le traitement automatisé de l'information. Cette pratique inquiétante est susceptible de causer des préjudices à des personnes innocentes, car des décisions seront prises à leur égard sans tenir compte du contexte, par la seule action d'un traitement automatique des données.

La protection des renseignements personnels, à une époque où ceux-ci circulent sans égard aux frontières nationales, constitue un enjeu majeur pour toute personne désireuse de demeurer maître de l'itinéraire que peuvent prendre ses renseignements personnels.

De manière générale, ce n'est pas tant la menace d'un État totalitaire que la Commission craint que l'avènement d'une surveillance de masse par la masse, c'est-à-dire de plusieurs organismes et personnes qui, à titre privé, se mettent à faire de la surveillance à des fins de sécurité.

Bien que la Commission traite souvent dans le présent avis des systèmes biométriques, de la vidéosurveillance et de l'IRF de façon séparée, ce choix méthodologique ne traduit pas la tendance de plus en plus forte à la convergence des diverses technologies de surveillance et de contrôle à des fins de sécurité. Déjà, les logiciels de reconnaissance faciale biométriques, l'introduction de données biométriques sur des puces d'IRF et autres hybrides laissent entrevoir le futur des systèmes de surveillance. Les effets, tant bénéfiques que néfastes, s'en trouveront vraisemblablement décuplés.

Étant donné que la tâche qui reste à accomplir pour encadrer de façon adéquate le déploiement des NTSC est considérable et que plusieurs actions dépassant le mandat de la Commission doivent être posées, celle-ci adresse une recommandation aux acteurs gouvernementaux en mesure de les accomplir.

La montée du sentiment d'insécurité, l'obsession pour l'élimination du risque et la sécurité ainsi que l'implantation de moyens de surveillance intrusifs sont des ingrédients nocifs pour la démocratie. Le déploiement des NTSC, s'il se fait en accord avec les valeurs fondamentales des sociétés démocratiques, peut contribuer à contrer ces menaces. Cependant, un juste équilibre doit être visé pour éviter que la surveillance par ces technologies ne mine à la base l'idéal démocratique : assurer un niveau jugé acceptable de sécurité sans bafouer les valeurs d'autonomie, de liberté, de vie privée et de transparence. Avec le présent avis, la Commission espère avoir ouvert un espace pour le dialogue sur les enjeux éthiques associés aux NTSC entre tous les acteurs concernés. Ses réflexions, ses prises de position et ses recommandations constituent sa contribution au débat public qu'elle souhaite voir s'amorcer.

Glossaire[236]

ADN – Macromolécule de poids moléculaire élevé, formée de polymères de nucléotides dont le sucre est le 2-désoxyribose, qui se présente sous forme d'une double chaîne hélicoïdale dont les deux brins sont complémentaires, et qui constitue le génome de la plupart des organismes vivants.

Chiffrement – Opération par laquelle est substitué, à un texte en clair, un texte inintelligible, inexploitable pour quiconque ne possède pas la clé permettant de le ramener à sa forme initiale.

Cybersurveillance – Ensemble de moyens de surveillance et de contrôle technique, sur une personne ou un processus, lié aux nouvelles technologies et plus particulièrement aux réseaux numériques de communication.

Forage des données – Technique de recherche et d'analyse de données, qui permet de dénicher des tendances ou des corrélations cachées parmi des masses de données, ou encore de détecter des informations stratégiques ou de découvrir de nouvelles connaissances en s'appuyant sur des méthodes de traitement statistique.

Géolocalisation – Dans le contexte de l'utilisation d'appareils mobiles, comme les téléphones cellulaires, ensemble des techniques qui permettent de déterminer leur position géographique, à partir des ondes radio qu'ils émettent.

Numérisation – Numérisation automatique, au moyen d'un numériseur à balayage, d'informations (texte ou image) présentées sous forme analogique.

Thermographie – Procédé permettant la visualisation et l'enregistrement du rayonnement thermique émis par l'organisme à travers la peau.

Victimisation – Attitude par laquelle un sujet se pose en victime, dans le but conscient ou inconscient de susciter chez autrui un sentiment de pitié ou même de culpabilité, et de se protéger ainsi contre toute accusation ou punition, tout en revendiquant indirectement la satisfaction de ses besoins matériels ou affectifs.

236. Sauf celle de la cybersurveillance, les définitions présentées dans le glossaire sont tirées du *Grand dictionnaire terminologique*. La définition de la cybersurveillance est tirée de Murielle CAHEN, « Le rôle de l'administrateur réseau dans la cybersurveillance », *netalya.com* [en ligne] [http://www.netalya.com/fr/Article2.asp?CLE=162].

Bibliographie*

« La biométrie faciale est-elle à la hauteur ? Le Bureau des passeports du Canada répond à la question », *III@L'OEUVRE*, été 2004.

« Les Canadiens et les Américains appuient l'application de la technologie biométrique pour les passeports et les permis de conduire : sondage », Communiqué de presse, Toronto, 2 août 2005.

« Research : World CCTV Market to Grow 37 Percent by 2009 », *SecurityInfoWatch.com* [en ligne], 14 juillet 2006. [http://www.securityinfowatch.com/online/Research--Studies-and-Whitepapers/8702SIW321].

« Sondage New York Times-CBS News », 17-21 août 2006.

AGRE, Philip E. *Your Face Is Not a Bar Code : Arguments against Automatic Face Recognition in Public* [en ligne], 10 septembre 2003. [http://polaris.gseis.ucla.edu/pagre/bar-code.html].

ASSOCIATION CANADIENNE DE L'ALARME ET DE LA SÉCURITÉ. *Pour un monde en toute sécurité*, mémoire présenté à la Commission d'accès à l'information, 2 septembre 2003.

ASSOCIATION SUR L'ACCÈS ET LA PROTECTION DE L'INFORMATION. *L'utilisation de caméras de surveillance par des organismes publics dans des lieux publics*, Mémoire soumis à la Commission d'accès à l'information dans le cadre de la consultation publique, septembre 2003.

BECK, Ulrich. *La société du risque : sur la voie d'une autre modernité*, Paris, Flammarion, 2001 (1986).

CAP GEMINI ERNST & YOUNG. *RFID and Consumers. Understanding Their Mindset. A U.S. Study Examining Consumer Awareness and Perceptions of Radio Frequency Identification Technology*, Executive Summary, 13 janvier 2004. [http://www.rfidconsultation.eu/docs/ficheiros/CPRD_RFID_mindset_ES.pdf].

CAVOUKIAN, Ann. *Biometrics and Policing : Comments from a Privacy Perspective*, Information and Privacy Commissioner/Ontario, août 1999.

CAVOUKIAN, Ann. *Guidelines for Using Video Surveillance Cameras in Public Spaces*, Information and Privacy Commissioner/Ontario, octobre 2001. [www.ipc.on.ca/images/Resources/video-e.pdf].

CAVOUKIAN, Ann. *Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines)*, Information and Privacy Commissioner/Ontario, juin 2006, p. 2. [www.ipc.on.ca/images/Resources/up-rfidgdlines.pdf].

CITOYENNETÉ ET IMMIGRATION CANADA. *Biométrie : incidences et applications pour la citoyenneté et l'immigration*, Document d'information, Forum tenu les 7 et 8 octobre 2003, Ottawa, Canada.

CITOYENNETÉ ET IMMIGRATION CANADA. *Biométrie : incidences et applications pour la citoyenneté et l'immigration*, Actes du forum tenu à Ottawa les 7 et 8 octobre 2003.

CLARK, Campbell. « Canadians Want Strict Security : Poll », *GlobeandMail.com* [en ligne], 11 août 2005. [http://www.theglobeandmail.com/servlet/story/RTGAM.20050811.wxsecurity11/BNStory/National/].

COMITÉ CONSULTATIF NATIONAL D'ÉTHIQUE POUR LES SCIENCES DE LA VIE ET DE LA SANTÉ. *Biométrie, données identifiantes et droits de l'homme*, Avis n° 98, 26 avril 2007. [www.comite-ethique.fr/docs/fr/avis098.pdf].

* Sauf mention particulière, toutes les adresses Internet étaient accessibles le 3 mars 2008, soit directement ou par le biais des archives de certains sites.

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. *Lignes directrices du Commissariat à la protection de la vie privée du Canada concernant le recours, par les forces policières et les autorités chargées de l'application de la loi, à la surveillance vidéo dans les lieux publics*, mars 2006. [http://www.privcom.gc.ca/information/guide/vs_060301_f.asp].

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC. *La biométrie au Québec : Les enjeux*, document d'analyse, juillet 2002. [http://www.cai.gouv.qc.ca/06_documentation/01_pdf/biom_enj.pdf].

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC. *La biométrie au Québec : Les principes d'application pour un choix éclairé*, juillet 2002.

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC. *La biométrie au Québec : les enjeux*, Document d'analyse, juillet 2002.

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC. *La technologie d'identification par radiofréquence (RFID) : doit-on s'en méfier ?*, Document d'analyse, mai 2006. [http://www.cai.gouv.qc.ca/06_documentation/01_pdf/Analyse_RFID.pdf].

COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE. *Pour une gestion éthique des OGM*, Sainte-Foy, 2003.

COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE. *L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques*, Document de réflexion, Sainte-Foy, 2005.

COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE. *L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques*, Document de consultation, Sainte-Foy, 2005.

COMMISSION EUROPÉENNE. *Protection des données dans l'Union européenne. Dialogue avec les citoyens et les entreprises*, guide sur la protection des données, 2000, Belgique.

COMMISSION EUROPÉENNE. *RFID Security, Data Protection and Privacy, Health and Safety Issues*, Policy Framework Paper [en ligne], 11 mai 2006. [http://www.rfidconsultation.eu/41/38/264.html].

COMMISSION EUROPÉENNE. *Your Voice on RFID. Background document for public consultation on Radio Frequency Identification (RFID) – Summary of five workshops*, juillet 2006. [http://www.rfidconsultation.eu/docs/ficheiros/Your_voice_on_RFID.pdf].

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. « La radio-identification », *cnil.fr* [en ligne], 30 juin 2006. [http://www.cnil.fr/index.php?id=1063].

COMPAS. *Terror after London*, BDO Dunwoody/Chamber Weekly CEO/Business Leader Poll by Compas in the *Financial Post*, 18 juillet 2005.

DANDEKER, Christopher. *Surveillance, Power and Modernity*, New York, St. Martin's Press, 1990, p. 37.

DELEURENCE, Guillaume. « Le passeport se convertit à l'électronique, avant la biométrie », *01net.com* [en ligne], 28 août 2006. [http://www.01net.com/editorial/324183/societe/le-passeport-se-convertit-a-l-electronique-avant-la-biometrie/].

DIONNE, Bernard et Évelyne RACETTE. « La biométrie : présentation à la Commission de l'éthique de la science et de la technologie », mars 2004 [manuscrit].

DUCE, Helen. *Executive Briefing, Public Policy : Understanding Public Opinion*, Auto-ID Centre, 1er février 2003. [http://www.autoidlabs.org/single-view/dir/article/6/199/page.html].

ELECTRONIC PRIVACY INFORMATION CENTER. « Radio Frequency Identification (RFID) Systems », *epic.org* [en ligne], 13 janvier 2006. [http://www.epic.org/privacy/rfid/].

ERICSON, Richard V. et Kevin D. HAGGERTY. *Policing the Risk Society*, Toronto, University of Toronto Press, 1997.

EWALD, François. *L'État providence*, Paris, Bernard Grasset, 1986.

FÉDÉRATION DES TRAVAILLEURS ET TRAVAILLEUSES DU QUÉBEC. *Mémoire de la Fédération des travailleurs et travailleuses du Québec présenté à la Commission d'accès à l'information du Québec sur l'utilisation de caméras de surveillance par des organismes publics dans les lieux publics*, Montréal, 22 septembre 2003. [http://www.ftq.qc.ca/modules/documents/index.php?id=5&langue=fr].

FERRY, Luc. « La nouvelle société du risque », dans *Liberté, risque & responsabilité : nouveaux repères à l'heure de la mondialisation et du terrorisme international*, Paris, Institut français des relations internationales, 2001.

FLAHERTY, David H. *Protecting Privacy in Surveillance Societies*, Chapel Hill, University of North Carolina Press, 1989.

FOSTER, Kenneth R. et Jan JAEGER. « RFID Inside. The Murky Ethics of Implanted Chips », *IEEE Spectrum*, mars 2007. [http://pages.cs.wisc.edu/~markhill/cs252/Spring2007/handouts/spectrum07_rfid_ethics.pdf].

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY. *Guide to Using Surveillance Cameras in Public Areas*, Gouvernement de l'Alberta, juin 2004. [http://foip.gov.ab.ca/resources/publications/pdf/SurveillanceGuide.pdf].

GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL DU PARLEMENT EUROPÉEN ET DU CONSEIL. *Document de travail sur les questions de protection des données liées à la technologie RFID (radio-identification)*, Bruxelles, 19 janvier 2005. [http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_fr.pdf].

GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL DE L'UNION EUROPÉENNE. *Document de travail sur la biométrie*, Bruxelles, Belgique, 1er août 2003.

HEMPEL, Leon et Eric TOPFER. *CCTV in Europe. Final Report*, Working Paper No. 15, août 2004. [http://www.urbaneve.net/results/ue_wp15.pdf].

HONESS, Terry et Elizabeth CHARMAN. *Closed Circuit Television in Public Places : Its Acceptability and Perceived Effectiveness*, Police Research Group, Crime Prevention Unit Series : Paper No. 35, Londres, Home Office Police Department.

IDTECHEX. *RFID Forecast, Players & Opportunities 2006-2016*, octobre 2006.

INDUSTRIE CANADA. « L'industrie canadienne de la sécurité : centres d'activité ».

INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES. *Biometrics at the Frontiers : Assessing the Impact on Society*, Technical Report Series, 2005, p. 39-40.

INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES, *Sécurité et respect de la vie privée du citoyen à l'ère du numérique après le 11 septembre : vision prospective*, Document de synthèse, Commission européenne, juillet 2003.

INTERNATIONAL BIOMETRIC GROUP, *Biometrics Market and Industry Report 2007-2012*.

INTERNATIONAL BIOMETRIC INDUSTRY ASSOCIATION. *IBIA Statement of Principles and Code of Ethics*, 23 octobre 2000. [http://www.ibia.org/aboutibia/ethics.asp].

JONAS, Hans. *Le principe responsabilité : une éthique pour la civilisation technologique*, Paris, Éditions du Cerf, 1990.

LAMALICE, Olivier. *Opinions publiques, incarcération et système pénal aux États-Unis : les influences de la classe politique et des médias*, document d'appoint préparé pour le ministère de la Sécurité publique. [http://www.msp.gouv.qc.ca/reinsertion/reinsertion.asp?txtSection=publicat].

LAPORTE, Michel. *Bilan*, Consultation publique : l'utilisation de caméras de surveillance par les organismes publics dans les lieux publics, Commission d'accès à l'information, avril 2004. [http://www.cai.gouv.qc.ca/06_documentation/01_pdf/bilan.pdf].

LE BRETON, David. *Sociologie du risque*, Paris, Presses Universitaires de France, 1995.

LEE, Murray. « Governing 'Fear of Crime' », dans Richard HIL et Gordon TAIT (dir.) *Hard Lessons*, Ashgate, Hants, 2004.

LÉGER MARKETING. *Les Canadiens et la sécurité au Canada*, 2002.

LÉGER MARKETING. *Le sentiment de sécurité des Canadiens*, janvier 2003.

LÉGER MARKETING. *Étude sur le sentiment de sécurité des Montréalais*, mars 2004.

LÉGER MARKETING. *Are Other Terrorist Attacks Imminent? September 11 from the Point of View of Canadians: 5 Years Later – Part 1*, août 2006.

LÉGER MARKETING. *Montréal une ville sécuritaire, attrayante mais malpropre*, février 2007.

LONDON SCHOOL OF ECONOMICS & POLITICAL SCIENCE. *The Identity Project. An Assessment of the UK Identity Cards Bill & Its Implications*, Department of Information Systems, 27 juin 2005.

LYON, David. *The Electronic Eye*, Minneapolis, University of Minnesota Press, 1994.

LYON, David. *Surveillance Society: Monitoring Everyday Life*, Buckingham, Open University Press, 2001.

MASSON, Isabelle. « Sécurité », Alex MACLEOD, Évelyne DUFAULT et F. Guillaume DUFOUR (dir.), *Relations internationales: théories et concepts*, Montréal, Athéna éditions, 2004.

MINISTÈRE DE LA SÉCURITÉ PUBLIQUE DU QUÉBEC. *Pour un Québec plus sécuritaire: partenaires en prévention*, Rapport de la Table ronde sur la prévention de la criminalité, 1993. [http://www.msp.gouv.qc.ca/prevention/prevention.asp?txtSection=publicat&txtCategorie=table_ronde].

MINISTÈRE DE LA SÉCURITÉ PUBLIQUE DU QUÉBEC. *Plan stratégique 2005-2008*, Gouvernement du Québec, 2005, p. 5.

NORRIS, Clive et Gary ARMSTRONG. *The Maximum Surveillance Society: The Rise of CCTV*, Oxford, Berg, 1999, p. 4.

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA. *Public Surveillance System Privacy Guidelines*, 26 janvier 2001. [http://www.oipcbc.org/advice/VID-SURV(2006).pdf].

OFFICE OF THE SASKATCHEWAN INFORMATION AND PRIVACY COMMISSIONER. *Guidelines for Video Surveillance by Saskatchewan Public Bodies*, 24 juin 2004. [www.oipc.sk.ca/webdocs/VideoSurveillance.pdf].

OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES. *Les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre*, Rapport présenté au Sénat par Christian Cabal, Assemblée nationale (France), juin 2003.

ORGANISATION DE DÉVELOPPEMENT ET DE COOPÉRATION ÉCONOMIQUES (OCDE). *Biometric-based Technologies*, Working Party on Information Security and Privacy, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy, Paris, 28 avril 2004.

ORGANISATION MONDIALE DE LA SANTÉ, *Sécurité et promotion de la sécurité: aspects conceptuels et opérationnels*, septembre 1998.

PARLEMENT EUROPÉEN ET CONSEIL DE L'EUROPE. *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques a l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, publiée dans le *Journal officiel*, n° L 281 du 23/11/1995, p. 0031 – 0050. [http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:FR:HTML].

PERETTI-WATEL, Patrick. *Sociologie du risque*, Paris, Armand-Colin, 2000.

PORTUGUESE DATA PROTECTION AUTHORITY. *Principles for the Use of Biometric Data in Controlling Access and Monitoring Hours Worked*, Portugal, 26 février 2004. [http://www.cnpd.pt/english/bin/guidelines/Guidelines%20biometric%20(EN).HTM].

PRIVACY INTERNATIONAL. *Overview of Privacy* [en ligne], 29 octobre 2006. [http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-543673&als[theme]=Privacy%20and%20Human%20Rights]

ROBIN, Corey. *Fear. The History of a Political Idea*, New York, Oxford University Press, 2004.

RODOTA, Stefano. « Privée (Protection de la vie) », dans Gilbert HOTTOIS et Jean-Noël MISSA (dir.), *Nouvelle encyclopédie de bioéthique*, Bruxelles, DeBoeck Université, 2001, p. 665-673.

SÆTNAN, Ann Rudinow, Heidi Mork LOMELL et Carsten WIECEK. « Controlling CCTV in Public Spaces: Is Privacy the (Only) Issue? Reflections on Norwegian and Danish observations », *Surveillance & Society*, vol. 2, nº 2/3, p. 396-414.

SCASSA, Teresa *et al. An Analysis of Legal and Technological Privacy Implications of Radio Frequency Identification Technologies*, préparé pour le Commissariat a la protection de la vie privée du Canada, 28 avril 2005.

SMITH, Gavin J.D. « Behind the Screens: Examining Constructions of Deviance and Informal Practices among CCTV Control Room Operators in the UK », *Surveillance & Society*, vol. 2, nº 2/3.

STATISTIQUE CANADA. *Enquête sociale générale sur la victimisation, cycle 18 : un aperçu des résultats*, Ottawa, Canada, 2004. [http://dsp-psd.pwgsc.gc.ca/Collection/Statcan/85-565-X/85-565-XIF.html].

STATISTIQUE CANADA. « Statistiques de la criminalité au Canada, 2005 », *Juristat*, vol. 26, nº 4, 20 juillet 2006.

STATISTIQUE CANADA. « Statistiques de la criminalité au Canada, 2006 », *Juristat*, vol. 27, nº 5, 18 juillet 2007.

STODDART, Jennifer. « Des technologies de surveillance sous surveillance », Discours [en ligne], septembre 2001. [http://www.cai.gouv.qc.ca/05_communiques_et_discours/discours_24_09_01.html].

STRATEGIC COUNSEL. *Immigration, Terrorism and National Security*, 7 août 2005.

STRATEGIC COUNSEL. *Public Perceptions of Immigration and Terrorism*, 9 juin 2006.

SURVEILLANCE STUDIES NETWORK. *A Report on the Surveillance Society*, Grande-Bretagne, septembre 2006. [http://www.ico.gov.uk/.../library/data_protection/practical_application/surveillance_society_full_report_2006.pdf].

THOMAS, Laurence. « Autonomie de la personne », *Dictionnaire d'éthique et de philosophie morale*, dans Monique CANTO-SPERBER (dir.), Paris, Presses Universitaires de France, 2001 (1996), p. 121-124.

BUREAU D'AUDIENCES PUBLIQUES SUR L'ENVIRONNEMENT. *Le projet de la Régie intermunicipale de gestion des déchets sur l'île de Montréal*, Rapport d'enquête et d'audience publique, 1993.

U.S. DEPARTMENT OF STATE. « Department of State Begins Issuing Electronic Passports to the Public », Communiqué de presse, 14 août 2006.

UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANISATION (UNESCO). *Ethical Implications of Emerging Technologies: A Survey*, Paris, UNESCO, 2007. [unesdoc.unesco.org/images/0014/001499/149992E.pdf].

WELSH, Brandon C. et David P. FARRINGTON. *Crime Prevention Effects of Closed Circuit Television: a Systematic Review*, Home Office Research Study 252, août 2002. [http://www.homeoffice.gov.uk/rds/pdfs2/hors252.pdf].

WOODWARD JR., John D. *et al. Army Biometric Applications: Identifying and Addressing Sociocultural Concerns*, RAND, 2001. [http://www.rand.org/publications/MR/MR1237/].

ZETTER, Kim. « Hackers Clone E-Passports », *Wired.com* [en ligne], 3 août 2006. [http://www.wired.com/science/discoveries/news/2006/08/71521].

ZUREIK, Elia, Lynda HARLING STALKER et Emily SMITH. *Background Paper for the Globalization of Personal Data Project: International Survey on Privacy and Surveillance*, Kingston, Queen's University, 2006.

Annexe 1

Les règles d'utilisation de la vidéosurveillance avec enregistrement dans les lieux publics par les organismes publics

Les éléments à considérer avant d'opter pour la vidéosurveillance

1) La vidéosurveillance doit être nécessaire à la réalisation d'une fin déterminée.

   Elle ne peut être utilisée de manière générale comme un dispositif de sécurité publique. Le problème à régler doit être identifié, récurrent et circonscrit.

2) L'objectif recherché par l'usage de la vidéosurveillance doit être sérieux et important.

   La prévention de délits mineurs ou la survenance de problèmes occasionnels ne peuvent justifier une intrusion dans la vie privée des personnes. La vidéosurveillance ne doit pas se révéler comme étant une solution de facilité. Les lieux ciblés doivent, notamment, être reconnus comme étant des espaces criminogènes.

3) Un rapport concernant les risques concrets et les dangers réels que présente une situation au regard de l'ordre public et de la sécurité des personnes, des lieux ou des biens doit être réalisé.

   Ce rapport doit notamment faire état des points suivants :

   - les événements précis, sérieux et concordants qui se sont produits ;
   - une identification claire du problème à régler ;
   - les exigences concrètes et réelles de sécurité publique en jeu ;
   - les lieux ciblés pour la vidéosurveillance et leurs liens avec les motifs invoqués ;
   - les objectifs importants, clairs et précis qui ont été identifiés.

4) Des solutions de rechange moins préjudiciables à la vie privée doivent avoir été envisagées ou mises à l'essai et s'être avérées inefficaces, inapplicables ou difficilement réalisables.

   Selon le problème à résoudre et les lieux concernés, d'autres solutions doivent avoir été expérimentées ou étudiées, notamment :

   - la présence d'agents de sécurité ;
   - une patrouille à pied aux endroits névralgiques ;
   - l'implication de travailleurs ou de travailleuses de rue ;
   - un service d'accompagnement à l'automobile sur demande ;
   - un meilleur éclairage de la zone à protéger (rues, parcs, corridors, etc.) ;
   - un renforcement des portes d'accès ;
   - l'installation de grilles protectrices et de systèmes d'alarme ou le marquage des objets reliés à un système d'alarme ;
   - une intervention du personnel de surveillance ;
   - la formation d'un comité de vigilance.

5) L'impact réel de la vidéosurveillance doit être mesuré.

Une analyse des risques au sujet de la protection de la vie privée a été complétée.

Les avantages et les inconvénients de la mesure doivent être soupesés, de même que ses effets potentiellement pervers ou non désirés, comme le déplacement de la criminalité. L'efficacité de la mesure pour corriger la situation doit être probante.

6) L'organisme public doit s'assurer de la légitimité de ses objectifs de sorte que la finalité de la vidéosurveillance ne puisse être détournée ou déformée.

Par exemple, la vidéosurveillance ne doit pas servir :

- à catégoriser ou hiérarchiser des groupes de personnes ;
- à établir des distinctions selon l'appartenance raciale, religieuse, politique ou syndicale ou les comportements sexuels des individus ;
- à étudier le comportement humain en vue d'exercer un contrôle sur ces personnes.

7) La finalité de la vidéosurveillance doit être transparente et explicite.

Les populations concernées doivent être consultées et impliquées avant la prise de décision. L'utilisation de la vidéosurveillance doit avoir été approuvée par les autorités imputables de l'organisme public.

8) La vidéosurveillance doit être considérée avec au moins un des éléments énoncés à la règle 4 ou son équivalent.

Les règles concernant la collecte des renseignements

9) L'organisme public doit désigner au départ une personne responsable de la collecte, de la conservation et de la communication des données recueillies au moyen de la vidéosurveillance.

Cette personne doit s'assurer, à toutes les étapes, que les présentes règles sont respectées.

10) La vidéosurveillance doit être ajustée au besoin et adaptée à la situation. L'organisme public doit circonscrire son usage.

Les périodes de surveillance et, éventuellement, d'enregistrement, l'espace visé et la manière dont se déroulera l'opération doivent être conçus de manière à minimiser les effets de la vidéosurveillance et à préserver le mieux possible la vie privée des citoyens.

11) La vidéosurveillance doit être utilisée uniquement lors d'événements critiques et pour des périodes limitées.

L'utilisation des caméras et l'enregistrement doivent être circonscrits à des heures de la journée et à des périodes de l'année précises correspondant aux moments forts ou se produisent habituellement les crimes. À titre d'exemple, s'il est établi que les infractions sont perpétrées la fin de semaine, en soirée ou la nuit, ou lors de fêtes publiques ou d'événements précis, la vidéosurveillance ne doit pas s'étendre au-delà de ces périodes.

12) Seuls les enregistrements nécessaires doivent être effectués.

Lorsqu'une personne peut visionner de façon permanente l'image captée par une caméra, elle doit attendre d'avoir des motifs raisonnables de croire qu'une infraction va être commise pour démarrer l'enregistrement.

Si personne ne peut visionner de façon continue les écrans, les bandes enregistrées doivent être détruites dès qu'elles ne sont plus nécessaires.

13) **La disposition des caméras et le type de technologie utilisée doivent minimiser les effets de la vidéosurveillance sur la vie privée des gens.**

Les caméras ne doivent pas être dirigées vers des endroits privés, tels une maison, des fenêtres d'immeubles, des salles de douche, les cabinets de toilette ou les vestiaires. À cette fin, la nouvelle technique informatique de masquage des lieux doit être retenue pour éviter une prise de vue d'endroits privés ou d'endroits qui ne sont pas concernés par la vidéosurveillance.

Les angles de vue, le type de caméras, la fonction zoom ou arrêt sur images doivent être évalués en fonction des finalités recherchées et des moyens appropriés pour atteindre ces finalités. Il en est de même de l'utilisation d'un équipement muni d'une connexion avec un centre d'alerte ou d'intervention.

14) **Les personnes assurant le fonctionnement des appareils doivent être bien au fait des règles visant à protéger la vie privée.**

Les personnes doivent avoir reçu la formation appropriée et connaître les limites imposées par la loi en matière de protection de la vie privée avant d'agir à titre d'opérateur. Il en va de même pour les tierces parties, soit celles ne relevant pas directement de l'autorité de l'organisme, notamment impliquées par contrat dans la vidéosurveillance.

15) **Le public visé par cette surveillance doit être informé par tout avis approprié.**

Des avis doivent annoncer de manière non équivoque que l'endroit fait l'objet de vidéosurveillance avec enregistrement.

Ces avis doivent :

- être placés à des endroits visibles, à une distance raisonnable du lieu surveillé et être d'un format requis par le contexte spatial ;
- mentionner l'objet de la vidéosurveillance et le nom de la personne responsable.

Les règles concernant la gestion des renseignements

16) **Les équipements utilisés pour l'enregistrement et les enregistrements doivent être protégés.**

Le matériel enregistré doit faire l'objet de règles précises de conservation en sorte que la confidentialité des données soit protégée.

Des mesures de sécurité doivent être mises en place afin de restreindre l'accès au poste de visionnement et aux enregistrements aux personnes expressément autorisées à cet effet.

Un nombre limité de personnes autorisées peuvent accéder aux locaux hébergeant les équipements et visionner les enregistrements.

17) **L'utilisation des enregistrements doit être limitée.**

Sous réserve des exceptions prévues à la Loi sur l'accès, les enregistrements ne doivent pas être communiqués à des tiers. À cet égard, l'interconnexion des systèmes de surveillance, que ce soit par Internet ou autrement, constitue une communication à un tiers.

Les enregistrements ne doivent pas faire l'objet d'associations d'images et de données biométriques, notamment à l'aide de logiciels de consultation automatique d'images ou de la reconnaissance faciale.

Les enregistrements ne doivent pas être appariés, couplés ou partagés avec d'autres fichiers, ni servir à constituer des banques de données.

18) Les supports d'enregistrement doivent être pris en compte dans le calendrier de conservation.

Les supports d'enregistrement doivent être numérotés et datés par site ayant fait l'objet d'une surveillance.

Mis à part les exigences judiciaires et les enquêtes policières ou administratives, les enregistrements sont effacés ou détruits dès que leur conservation n'est plus nécessaire.

19) Une personne a droit d'accès aux renseignements la concernant.

Cette personne a droit d'accès aux enregistrements effectués conformément à la Loi sur l'accès.

La révision périodique de la décision de recourir à la vidéosurveillance

20) L'organisme public doit revoir périodiquement (au minimum sur une base annuelle) la nécessité de ses choix en matière de vidéosurveillance.

À cet effet, les aspects suivants doivent être pris en considération :

- les motifs de départ existent toujours ;
- les résultats escomptés sont atteints. Sinon, l'organisme public doit s'interroger sur les effets réels du procédé ;
- les conditions d'utilisation sont toujours adéquates et adaptées à la situation ;
- la pertinence du type de caméras utilisées ainsi que leur nombre ;
- une solution de rechange plus appropriée et compatible avec le droit au respect de la vie privée n'est pas maintenant envisageable ;
- le cas échéant, le nombre d'heures d'enregistrement par jour ainsi que des périodes d'enregistrement pendant la semaine ou l'année.

Commission d'accès à l'information du Québec

Annexe 2

Lignes directrices du Commissariat à la protection de la vie privée du Canada concernant le recours, par les forces policières et les autorités chargées de l'application de la loi, à la surveillance vidéo dans les lieux publics

1) La surveillance vidéo devrait être utilisée seulement pour traiter un problème réel, urgent et important.

Le problème à régler au moyen de la surveillance vidéo doit être urgent et sérieux, suffisamment important pour justifier une dérogation au droit des personnes innocentes de ne pas être surveillées dans un lieu public. Par conséquent, il faut bien démontrer qu'il y a un problème à régler, notamment par une étude des risques et des dangers, le taux de criminalité, etc. On doit présenter des rapports précis et vérifiables d'actes criminels ou faire valoir des préoccupations relatives à la sécurité publique ou d'autres circonstances qui l'exigent ; on ne peut simplement fournir des renseignements empiriques ou avancer des hypothèses.

2) La surveillance vidéo devrait demeurer une mesure exceptionnelle, à utiliser uniquement à défaut d'autres moyens portant moins atteinte à la vie privée.

Pour régler un problème donné, il convient de choisir les moyens portant le moins atteinte à la vie privée, sauf s'ils sont impossibles à mettre en place ou beaucoup moins efficaces.

3) Avant d'entreprendre la surveillance vidéo proposée, il faudrait évaluer ses incidences sur la vie privée.

L'incidence sur la vie privée de la surveillance vidéo proposée doit être évaluée afin de déterminer le type et le degré d'atteinte réelle ou possible à la vie privée qui en résultera, ainsi que les moyens prévus pour en atténuer les effets négatifs.

4) Toute décision visant à recourir à la surveillance vidéo devrait reposer sur des consultations publiques.

Des consultations publiques devraient être menées auprès d'intervenants pertinents, notamment les représentants des communautés visées. Le terme « communauté » s'entend ici au sens large ; il est important de reconnaître qu'une zone géographique peut compter plusieurs communautés distinctes et de ne pas présumer qu'une d'entre elles parle au nom des autres.

5) La surveillance vidéo devrait être conforme aux lois applicables.

La surveillance vidéo doit s'effectuer conformément aux lois applicables, y compris les lois générales comme la Charte canadienne des droits et libertés et la Charte québécoise des droits et libertés de la personne.

6) Le système de surveillance vidéo devrait être conçu de manière à limiter les incidences sur la vie privée.

Le système de surveillance doit être conçu et utilisé de façon à ce que l'atteinte à la vie privée ne soit pas plus élevée que celle qui est absolument nécessaire pour réaliser les objectifs du système. Par exemple, il faut privilégier le recours restreint à la surveillance vidéo (p. ex., à certaines heures du jour, aux festivals publics, aux périodes de pointe) à une surveillance continue, si le résultat atteint est à peu près le même.

7) **Le public devrait être informé de la surveillance dont il fera l'objet.**

Dans le périmètre de la zone de surveillance, le public doit être informé par des panneaux qu'il se trouve dans une zone surveillée ou susceptible de l'être ; il doit pouvoir y lire qui est responsable de cette mesure, y compris la personne chargée du respect des principes de protection de la vie privée et la personne à contacter s'il a des questions ou s'il désire de l'information sur le système.

8) **Des pratiques équitables de traitement de l'information devraient être suivies lors de la collecte, de l'utilisation, de la communication, de la conservation et de la destruction de renseignements personnels.**

Les renseignements personnels recueillis au moyen de la surveillance vidéo doivent être restreints au minimum ; il faut en limiter l'utilisation, en contrôler la communication, en restreindre la période de conservation et en assurer la destruction. Si une caméra fonctionne sous la supervision d'un employé, elle ne doit enregistrer des images que dans les cas où on a constaté une infraction ou qu'on en soupçonne une. Si elle est continuellement en marche, il faut garder les enregistrements pendant une période de temps limitée, conformément à un calendrier de conservation, à moins qu'elle ait saisi des images d'infraction soupçonnée ou se rapportant à un acte criminel signalé à la police. Les renseignements recueillis par la surveillance vidéo ne doivent pas servir à d'autres fins que celles énoncées explicitement par le corps policier ou l'autorité publique dans la politique énoncée au point 14 ci-après. Toute communication d'enregistrements doit être documentée.

9) **Les intrusions excessives ou non nécessaires dans la vie privée devraient faire l'objet de dissuasion.**

Les caméras de surveillance ne doivent pas être dirigées vers des endroits où les gens s'attendent le plus au respect de leur vie privée, notamment les fenêtres d'immeubles, les salles de douches, de toilettes, d'essayage, etc. Si les caméras sont orientables par un opérateur, il convient de prendre des mesures raisonnables pour qu'il lui soit impossible de les orienter ou de les manipuler afin de saisir des images dans des zones non visées par la surveillance.

10) **Les opérateurs de systèmes de surveillance devraient être au fait des règles relatives à la protection de la vie privée.**

Les opérateurs de systèmes de surveillance, y compris les contractuels, doivent bien comprendre les objectifs du système et avoir reçu une formation complète sur les règles de protection de la vie privée.

11) **La sécurité du matériel et des images devrait être assurée.**

L'accès aux contrôles et au matériel de réception du système, ainsi qu'aux images saisies par ce dernier, devra être réservé aux personnes autorisées par écrit aux termes de la politique énoncée au point 14 ci-après. Les enregistrements doivent être conservés de façon sécuritaire, tout comme l'accès au sein de l'organisme doit se limiter aux cas de nécessité absolue.

12) **Le droit des personnes d'avoir accès à leurs renseignements personnels devrait être respecté.**

Les gens dont les images sont enregistrées doivent pouvoir avoir accès sur demande aux renseignements personnels qui les concernent. En vertu de nombreuses lois sur la protection des renseignements personnels, ils disposent d'un droit d'accès. Il peut être nécessaire de retrancher des renseignements personnels d'un enregistrement (notamment l'identité des autres personnes par brouillage ou blocage technologique) pour permettre l'accès aux enregistrements en question. Les politiques et les procédures doivent être conçues de façon à pouvoir répondre à ces demandes.

13) **Le système de surveillance vidéo devrait faire l'objet d'une vérification et d'une évaluation indépendantes.**

Il faut vérifier fréquemment le fonctionnement du système et évaluer régulièrement son efficacité pour en cerner les effets indésirables. Il incombe à des personnes ou à des organisations non associées à la gestion ou à la direction du système de surveillance vidéo de procéder à la vérification et à l'évaluation. Lors de la vérification,

on s'assure que la politique régissant le système est respectée, que seuls les renseignements pertinents sont recueillis, que le système sert uniquement aux fins prévues et que les mesures du système pour la protection de la vie privée sont suivies. L'évaluation précise les raisons justifiant la surveillance en premier lieu, telles qu'elles ont été déterminées dans la formulation du problème et lors de la consultation publique. Elle doit aussi indiquer si la surveillance vidéo a permis de régler le problème cerné au cours de ces étapes. L'évaluation peut déterminer que le système doit être enlevé, si le problème cerné au départ n'est plus pertinent ou si la surveillance n'a pas été efficace pour régler le problème. L'évaluation présente aussi les points de vue des différents groupes au sein de la communauté (ou des différentes communautés) touchée par la surveillance. Le public doit pouvoir avoir accès aux résultats des vérifications et des évaluations.

14) **Une politique explicite devrait régir le recours à la surveillance vidéo.**

Une politique écrite complète régissant l'utilisation de matériel de surveillance doit être élaborée. Elle doit énoncer clairement :

- la justification et l'objectif du système
- l'emplacement et le champ de vision du matériel
- la justification et l'objectif de l'emplacement et du champ de vision choisis
- le personnel autorisé à opérer le système
- les heures de surveillance
- le moment où l'enregistrement a lieu, le cas échéant
- l'endroit où ont lieu la réception et la surveillance des signaux du matériel
- les principes relatifs à l'équité dans le traitement des renseignements qui s'appliquent aux enregistrements, notamment :
  - la sécurité
  - l'utilisation
  - la communication
  - la conservation et la destruction
  - les droits des personnes d'avoir accès aux renseignements personnels recueillis
  - le droit de contester la conformité.

La politique doit indiquer qui est responsable de la conformité et du droit à la protection de la vie privée associé associés? [*sic*] au système. Elle doit aussi exiger des agents, employés et entrepreneurs qu'ils s'y conforment et prévoir des sanctions dans le cas contraire. Elle doit comporter un processus à suivre dans l'éventualité d'un manquement par inadvertance à la protection des renseignements personnels et à la sécurité. Enfin, elle doit énoncer une procédure pour les personnes qui désirent la remettre en question.

15) **Le public devrait avoir le droit d'être informé au sujet du système de surveillance vidéo qui a été adopté.**

Le corps policier et les autorités publiques doivent reconnaître que les personnes voudront de l'information sur les systèmes de surveillance vidéo utilisés. Ces dernières peuvent chercher à savoir, par exemple, qui a autorisé l'enregistrement, si des images d'elles ont été saisies et pourquoi, à quoi ces images vont servir, qui y aura accès et combien de temps elles seront conservées. Le corps policier et les autorités publiques doivent être prêts à fournir ces renseignements.

Commissariat à la protection de la vie privée du Canada

Les activités de consultation et d'information de la Commission

Experts entendus dans le cadre de présentations au comité de travail

M. Daniel Carpentier, conseiller juridique à la Direction de la recherche et de la planification, Commission des droits de la personne et des droits de la jeunesse (CDPDJQ)

M^me^ Sylvie Laflamme, Directrice administrative du chapitre du Québec, Association canadienne de la sécurité (CANASA)

M. Sylvain Lemay, Inspecteur, Division de la qualité des services, Service de police de la Ville de Montréal (SPVM)

M. Bruno Leclerc, professeur, Département des sciences humaines, programmes d'études supérieures en éthique, Université du Québec à Rimouski (UQAR) ; directeur du groupe de recherche Ethos

M. André Beauchamp, consultant en environnement

M^me^ Julie-Anne Boudreau, professeure-chercheuse, INRS – Urbanisation, Culture et Société ; titulaire de la Chaire de recherche du Canada sur la ville et les enjeux politiques liés à l'insécurité

En décembre 2007, les personnes suivantes ont accepté de procéder à une lecture critique d'une première version du rapport du comité de travail

M. Jean-Philippe Racicot, analyste, Bureau du Conseil privé

M. Sami Aoun, professeur titulaire, École de politique appliquée, Faculté des lettres et sciences humaines, Université de Sherbrooke

M. Daniel Carpentier, conseiller juridique à la Direction de la recherche et de la planification, Commission des droits de la personne et des droits de la jeunesse du Québec (CDPDJQ)

M. Clément Robitaille, ministère de la Sécurité publique (MSP)

M. Hervé Fischer, professeur associé, Université du Québec à Montréal (UQAM) ; fondateur et directeur, Observatoire international du numérique

M. Patrice St-Gelais, conseiller en technologies de l'information, Commission d'accès à l'information (CAI)

La Commission remercie toutes ces personnes pour la collaboration qu'elles ont apportée à sa réflexion et à l'enrichissement du contenu de son avis.

Participation à des événements

- *Terra Incognita, Les horizons de la protection de la vie privée*, 29^e^ Conférence internationale des commissaires à la protection des données et de la vie privée, du 25 au 28 septembre 2007, Montréal.

Liste des membres de la Commission[237]

Présidente

Me Édith Deleury
Professeure – Faculté de droit
Université Laval

Membres

Frédéric Abraham
Doctorant en philosophie
Université du Québec à Trois-Rivières

Patrick Beaudin
Directeur général
Société pour la promotion de la science
et de la technologie

Dr Pierre Deshaies
Médecin spécialiste en santé communautaire
Chef du Département clinique de santé publique
Hôtel-Dieu de Lévis

Hubert Doucet
Programmes de bioéthique
Université de Montréal

Benoit Gagnon
Chercheur
Centre international de criminologie comparée (CICC)
Université de Montréal

Jacques T. Godbout
Sociologue
Institut national de la recherche scientifique –
Urbanisation, Culture et Société

Patrice K. Lacasse
Coordonnateur du Bureau de développement social
des Premières Nations du Québec
Commission de la santé et des services sociaux
des Premières Nations du Québec et du Labrador

François Pothier
Professeur
Faculté des sciences de l'agriculture et de l'alimentation
Université Laval

Dany Rondeau
Professeure
Département des sciences humaines
Université du Québec à Rimouski

Andy Sheldon
Président et chef de la direction
Medicago inc.

Eliana Sotomayor
École de service social
Université de Montréal

Membre invitée

Me Danielle Parent
Directrice des affaires juridiques
Commissaire au lobbyisme du Québec

Coordonnatrice

Me Nicole Beaudry, notaire

237. Au moment de l'adoption de l'avis.

La surveillance de masse peut être considérée comme un trait caractéristique des sociétés modernes. Son importance n'a d'égal que les moyens mis en place pour amasser des renseignements. Parmi ces moyens, les nouvelles technologies de surveillance et de contrôle (NTSC) et surtout les manières de les déployer soulèvent des enjeux éthiques. Aussi, la Commission de l'éthique de la science et de la technologie s'est-elle donné le mandat de formuler un avis sur des technologies pouvant servir à la surveillance de masse à des fins de sécurité : les systèmes biométriques, la vidéosurveillance et l'identification par radiofréquence (IRF).

Viser un juste équilibre : un regard éthique sur les nouvelles technologies de surveillance et de contrôle à des fins de sécurité est le cinquième avis de la Commission. Après s'être intéressée aux notions de sécurité, de sentiment d'insécurité, de risque et de surveillance, la Commission fait un tour d'horizon des aspects techniques et éthiques de chacune des NTSC retenues. Les valeurs fondamentales au sein des sociétés démocratiques s'inscrivent au cœur des enjeux éthiques traités : l'évaluation de la pertinence, de l'efficacité et de la fiabilité des NTSC, la proportionnalité de la réponse à l'insécurité, l'acceptabilité sociale, le consentement, le respect des finalités et la protection des renseignements personnels.

Pour en savoir plus sur la Commission et ses publications, visitez son site à l'adresse suivante : www.ethique.gouv.qc.ca

La mission de la Commission de l'éthique de la science et de la technologie consiste, d'une part, à informer, sensibiliser, recevoir des opinions, susciter la réflexion et organiser des débats sur les enjeux éthiques du développement de la science et de la technologie, et, d'autre part, à proposer des orientations susceptibles de guider les acteurs concernés dans leur prise de décision.

Commission
de l'éthique
de la science
et de la technologie
Québec